Lecture Notes in Algebraic Number Theory

Lectures by Dr. Sheng-Chi Liu

Throughout these notes, □ signifies end proof, and ▲ signifies end of example.

Table of Contents

Notes by Jakob Streipel. Last updated June 13, 2021.

Lecture 1 Review

Algebraic number theory is fundamentally the study of finite extensions of the rational numbers $\mathbb{Q}$, called number fields. To this end we will first review some of the theory of field extensions.

1.1 Field Extensions

Definition 1.1.1 (Finite field extension)**.** A ***finite field extension*** of a field K is a field $L \supset K$ such that $\dim_K L$ is finite (as a vector space over K).

The ***degree*** of the extension L/K is defined to be $\deg(L/K) \coloneqq \dim_K L$.

Fact. *If we have a tower of finite field extensions, say $K \subset L \subset F$, then $\deg(F/K) = \deg(F/L) \cdot \deg(L/K)$.*

The proof of this boils down to considering a basis of either extension and expressing one with the help of the other, and the amount of elements in the basis between F and K will be the product of the number of basis elements in either intermediate extensions.

Definition 1.1.2 (Algebraic element)**.** Let L/K be a field extension, and let $\alpha \in L$. Then α is called ***algebraic*** over K if it satisfies $f(\alpha) = 0$ for some $f \in K[x]$.

Fact. *Any element of a finite extension of K is algebraic over K.*

To see this, consider an extension $L \supset K$ of degree n and let $\alpha \in L$. Then $1, \alpha, \alpha^2, \ldots, \alpha^n$ are linearly dependent in K, since there are more than n of them, and therefore there is a nontrivial linear combination over K of them that adds to 0, which in turn gives us a polynomial in $K[x]$ with α as a root.

Fact. *An algebraic element $\alpha \in L$ has a minimal polynomial over K, i.e. there exists a unique $p_\alpha(x) \in K[x]$ such that if $f(x) \in K[x]$ with $f(\alpha) = 0$, then $p_\alpha(x) \mid f(x)$, with the uniqueness being up to multiplication by an element in K.*

Equivalently, therefore, there is a unique monic polynomial of least degree with α as its root.

Fact. *For an algebraic element $\alpha \in L$ with minimal polynomial $p_\alpha(x)$, we have the isomorphism*

$$K(\alpha) \cong \frac{K[x]}{\langle p_\alpha(x) \rangle},$$

with the isomorphism being the map that evaluates x in α. Moreover

$$\deg(K(\alpha)/K) = \deg(p_\alpha(x)) = n$$

and $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ is a bases for $K(\alpha)$ over K. Thus $K(\alpha) = K[\alpha]$, and in the latter α^n and higher degrees can be reduced to lower degrees.

Definition 1.1.3 (Number field)**.** An (algebraic) ***number field*** K ($\subset \mathbb{C}$) is a finite extension of $\mathbb{Q}$.

Date: January 9th, 2018.

Theorem 1.1.4 (Primitive element theorem)**.** *Let K be a number field. Then $K = \mathbb{Q}(\alpha) = \mathbb{Q}[\alpha]$ for some $\alpha \in K$.*

Two famous examples of number fields are the following:

Example 1.1.5 (Quadratic fields)**.** Consider $K = \mathbb{Q}(\sqrt{D})$, where D is a square-free integer (otherwise, simply pull out the square part). If $D > 0$, then $\mathbb{Q}(\sqrt{D})$ is called a ***real quadratic field***, and if $D < 0$ then $\mathbb{Q}(\sqrt{D})$ is an ***imaginary quadratic field***.

These extensions are of degree 2, since the minimal polynomial of $\sqrt{D}$ is $x^2 - D$, and moreover they are Galois extensions since they are both separable and normal. ▲

Example 1.1.6 (Cyclotomic fields)**.** Consider $K = \mathbb{Q}(\xi_m)$, where ξ_m is a ***primitive mth root of unity***, meaning that $\xi_m^m = 1$ and $\xi_m^n \neq 1$ for $0 < n < m$. For instance, and by convention what we'll always use, $\xi_m = e^{2\pi i/m}$. The other primitive mth roots of unity are ξ_m^k where $\gcd(m, k) = 1$, so $\deg(K/\mathbb{Q}) = \varphi(m)$, where by φ we mean Euler's totient function.

Note that if $m = 1$, $\xi_1 = 1$ and if $m = 2$ we have $\xi_2 = -1$, so $K = \mathbb{Q}$ in both cases, making neither of these interesting. Hence when discussing cyclotomic fields we are interested in $m \geq 3$, since when $m = 3$ we get $\xi_3 = e^{2\pi i/3}$ yielding $K = \mathbb{Q}(\xi_3)$ which is an extension of degree $\varphi(3) = 2$.

Now if $m = 6$, then $\xi_6 = -\xi_6^4 = -(\xi_6^2)^2$, by straight forward computation, meaning that $\mathbb{Q}(\xi_6^2) = \mathbb{Q}(\xi_6)$, but note that $\xi_6^2 = \xi_3$, so in fact $\mathbb{Q}(\xi_3) = \mathbb{Q}(\xi_6)$. ▲

This last idea generalises:

Proposition 1.1.7. *For odd m, $\mathbb{Q}(\xi_m) = \mathbb{Q}(\xi_{2m})$.*

Proof. Take $\xi_m = e^{2\pi i/m}$ and likewise $\xi_{2m} = e^{2\pi i/(2m)}$. Then clearly $\xi_{2m}^2 = \xi_m$, so $\mathbb{Q}(\xi_m) = \mathbb{Q}(\xi_{2m}^2) \subset \mathbb{Q}(\xi_{2m})$.

On the other hand, $\xi_{2m}^m = e^{\pi i} = -1$, meaning that $\xi_{2m}^{m+1} = -\xi_{2m}$. Since m is odd, $m + 1$ is even, and therefore $\xi_{2m}^{m+1} = -\xi_{2m} \in \mathbb{Q}(\xi_{2m}^2)$, implying that $\mathbb{Q}(\xi_{2m}) \subset \mathbb{Q}(\xi_{2m}^2) = \mathbb{Q}(\xi_m)$. □

Remark 1.1.8. We will show that for even m, all $\mathbb{Q}(\xi_m)$ are distinct. Note also that $\mathrm{Gal}(\mathbb{Q}(\xi_m)/\mathbb{Q}) \cong (\mathbb{Z}/m\mathbb{Z})^\times$.

Definition 1.1.9 (Algebraic integer)**.** An element $\alpha \in \mathbb{C}$ is called an ***algebraic integer*** if it is a root of a monic polynomial $f(x) \in \mathbb{Z}[x]$.

Example 1.1.10. Many elements are algebraic integers. For instance, $\sqrt{2}$ is, since its minimal polynomial is $x^2 - 2$, which is monic. Similarly 5 is an algebraic integer, since it is the root of $x - 5$, and $\sqrt{D}$ is the root of $x^2 - D$.

The primitive roots of unity are too, since ξ_m is a root of $f(x) = x^m - 1$. ▲

This notion is equivalent with the notion from commutative algebra of α being integral over $\mathbb{Z}$.

Note also that since there are only countably many polynomials over $\mathbb{Z}$, the fundamental theorem of algebra implies that there are only countably many algebraic integers.

Theorem 1.1.11. *The following are equivalent for $\alpha \in \mathbb{C}$:*

(*i*) α *is an algebraic integer.*

(*ii*) $\mathbb{Z}[\alpha]$ *is a finitely generated* $\mathbb{Z}$*-module (i.e. Abelian group).*

(*iii*) *There exists a subring of* $\mathbb{C}$ *containing* α *that is finitely generated.*

(*iv*) *There exists a finitely generated nonzero* $\mathbb{Z}$*-module* $M \subset \mathbb{C}$ *such that* $\alpha M \subset M$*.*

Proof. That (*i*) implies (*ii*) is clear: since α is an algebraic integer we have an equation

$$\alpha^n + c_{n-1}\alpha^{n-1} + \ldots + c_1\alpha + c_0 = 0$$

for some $c_i \in \mathbb{Z}$. Rearranging this for α^n we have

$$\alpha^n = -(c_{n-1}\alpha^{n-1} + \ldots + c_1\alpha + c_0)$$

meaning that $\mathbb{Z}[\alpha]$ is finitely generated by $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$.

(*ii*) trivially implies (*iii*) by just taking $\mathbb{Z}[\alpha]$ itself, and in the same way (*iii*) implies (*iv*) using the subring from (*iii*) itself.

Finally (*iv*) implies (*i*) by letting $x_1, x_2, \ldots, x_n$ be generators of M, and since $\alpha M \subset M$, we have

$$\alpha x_i = a_{i1}x_1 + a_{i2}x_2 + \ldots + a_{in}x_n$$

for all $i = 1, 2, \ldots, n$, with $a_{ij} \in \mathbb{Z}$. As matrix equations we then have

$$\begin{pmatrix} \alpha x_1 \\ \alpha x_2 \\ \vdots \\ \alpha x_n \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix},$$

which rearranged and calling the coefficient matrix A and the x_i-vector x, that $(\alpha I_n - A)x = 0$, where I_n is the identity matrix. Now since $x_1, x_2, \ldots, x_n$ generate a nontrivial $\mathbb{Z}$-module, $x \neq 0$, so $(\alpha I_n - A)$ has linearly dependent columns, making its determinant 0, so

$$0 = \det(\alpha I_n - A) = \alpha^n + \text{lower order terms in } \alpha. \qquad \square$$

Corollary 1.1.12. *Let* A *be the set of algebraic integers in* $\mathbb{C}$*. Then* A *is a ring.*

Proof. We need to show that $\alpha + \beta$ and $\alpha\beta$ are both in A if α and β are in A. This follows almost trivially from the above theorem, however: we have that $\mathbb{Z}[\alpha]$ and $\mathbb{Z}[\beta]$ are finitely generated $\mathbb{Z}$-modules, and therefore $\mathbb{Z}[\alpha, \beta]$ is finitely generated as a $\mathbb{Z}$-module as well. This latter ring contains $\alpha + \beta$ and $\alpha\beta$, and therefore they are algebraic integers. $\square$

Definition 1.1.13. Let K be a number field. The ***ring of integers*** $\mathcal{O}_K$ of K is the set of algebraic integers in K, i.e. $\mathcal{O}_K = A \cap K$.

By the above corollary, it is a subring of K. Note also that in the language of commutative algebra, this makes $\mathcal{O}_K$ the integral closure of $\mathbb{Z}$ in K, meaning in particular that $\mathcal{O}_K$ is integrally closed.

Theorem 1.1.14. *Let K be a number field, and let $\alpha \in K$. Then α can be written as $\alpha = \beta/d$, where $\beta \in \mathcal{O}_K$ and $d \in \mathbb{Z}$. Hence K is the quotient field of $\mathcal{O}_K$.*

Proof. Since $\alpha \in K$ is algebraic over $\mathbb{Q}$ we have

$$\alpha^n + c_{n-1}\alpha^{n-1} + \ldots + c_1\alpha + c_0 = 0$$

with $c_i \in \mathbb{Q}$. We can write all of the fractions c_i with common denominator, say $c_i = b_i/d$, with $b_i, d \in \mathbb{Z}$, and $d \neq 0$. Hence

$$\alpha^n + \frac{b_{n-1}}{d}\alpha^{n-1} + \ldots + \frac{b_i}{d}\alpha + \frac{b_0}{d} = 0.$$

Multiplying this by d^n we get

$$(d\alpha)^n + b_{n-1}(d\alpha)^{n-1} + \ldots + b_1 d^{n-2}(d\alpha) + b_0 d^{n-1} = 0,$$

which we can interpret as a monic polynomial in $d\alpha$, meaning that $d\alpha = \beta \in \mathcal{O}_K$, and so $\alpha = \beta/d$. □

Lecture 2 Ring of Integers

2.1 Understanding Algebraic Integers

Recall that α is an algebraic integer, or integral over $\mathbb{Z}$, if $f(\alpha)$ for some monic $f(x) \in \mathbb{Z}[x]$.

The question with which we will concern ourselves for the foreseeable future is this: what is $\mathcal{O}_K$ if K is, say, $\mathbb{Q}$, $\mathbb{Q}(\sqrt{D})$, or $\mathbb{Q}(\xi_m)$. The answers, respectively, are $\mathbb{Z}$, depends on whether $D \equiv 1 \pmod 4$, and $\mathbb{Z}[\xi_m]$. We will spend some time proving these claims.

Theorem 2.1.1. *Let α be an algebraic integer. Let $f(x) \in \mathbb{Z}[x]$ be a monic polynomial of least degree such that $f(\alpha) = 0$. (Note that this implies that f is irreducible over $\mathbb{Z}$.)*

Then $f(x)$ is irreducible over $\mathbb{Q}$.

We will prove this in a moment, but first note the following straight-forward corollary:

Corollary 2.1.2. *The number α is an algebraic integer if and only if the monic minimal polynomial of α over $\mathbb{Q}$ has coefficients in $\mathbb{Z}$.*

Proof. The latter implying the former is true by definition, and the former implying the latter is the above theorem. □

We will use the following result to prove the theorem:

Lemma 2.1.3 (Gauss Lemma)**.** *Let $f(x) \in \mathbb{Z}[x]$ be a monic polynomial. Suppose $f(x) = g(x)h(x)$ with $g(x), h(x) \in \mathbb{Q}[x]$ monic. Then $g(x), h(x) \in \mathbb{Z}[x]$.*

More generally, we can replace $\mathbb{Z}$ by any unique factorisation domain and $\mathbb{Q}$ by its field of fractions.

Date: January 11th, 2018.

Proof. Let m and n be the *smallest* positive integers such that $mg(x)$ and $nh(x)$ have coefficients in $\mathbb{Z}$. Hence the coefficients of $mg(x)$ have no common factors, and the same is true for the coefficients of $nh(x)$.

We claim that $m = n = 1$.

Suppose not, i.e. $mn > 1$. Take a prime p such that $p \mid mn$, and consider $mnf(x) = (mg(x))(nh(x))$. Reducing this modulo p we get $0 = \overline{mg(x)} \cdot \overline{nh(x)} \in \mathbb{Z}/p\mathbb{Z}[x]$. Now $\mathbb{Z}/p\mathbb{Z}$ is a field, which in particular makes it an integral domain, so the polynomial ring is an integral domain too. Hence $\overline{mg(x)} = 0$ or $\overline{nh(x)} = 0$.

Therefore p divides all coefficients of $mg(x)$, or p divides all coefficients of $nh(x)$, which is a contradiction since we chose m and n minimal in order to make sure the coefficients had no common factors. □

Using this we are equipped to prove the theorem:

Proof of 2.1.1. Suppose $f(x)$ is reducible over $\mathbb{Q}$, i.e. $f(x) = g(x)h(x)$, where $g(x), h(x) \in \mathbb{Q}[x]$. Since $f(x)$ is monic and since $\mathbb{Q}$ is a field, we can assume without loss of generality that g and h are monic too. Gauss Lemma therefore implies that $g(x), h(x) \in \mathbb{Z}[x]$.

Moreover $\deg g, \deg h < \deg f$, but since $0 = f(\alpha) = g(\alpha)h(\alpha)$ implies that $g(\alpha) = 0$ or $h(\alpha) = 0$, we have a contradiction, for f was chosen to be of minimal degree with α as a zero. □

Corollary 2.1.4. *The only algebraic integers in $\mathbb{Q}$ is $\mathbb{Z}$.*

Proof. The minimal monic polynomial of $\alpha \in \mathbb{Q}$ over $\mathbb{Q}$ is $f(x) = x - \alpha$, naturally. Now α is an algebraic integer if and only if $f(x) \in \mathbb{Z}[x]$, if and only if $\alpha \in \mathbb{Z}$. □

We are now ready to find the ring of integers for quadratic integers.

Corollary 2.1.5. *Consider $K = \mathbb{Q}(\sqrt{D})$, with D being square-free. Then*

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}[\sqrt{D}] = \{\, a + b\sqrt{D} \mid a, b \in \mathbb{Z} \,\}, & \text{if } D \not\equiv 1 \pmod 4, \\ \mathbb{Z}[\frac{1+\sqrt{D}}{2}] = \{\, a + b\frac{1+\sqrt{D}}{2} \mid a, b \in \mathbb{Z} \,\}, & \text{if } D \equiv 1 \pmod 4. \end{cases}$$

Proof. Let

$$R = \begin{cases} \mathbb{Z}[\sqrt{D}] = \{\, a + b\sqrt{D} \mid a, b \in \mathbb{Z} \,\}, & \text{if } D \not\equiv 1 \pmod 4, \\ \mathbb{Z}[\frac{1+\sqrt{D}}{2}] = \{\, a + b\frac{1+\sqrt{D}}{2} \mid a, b \in \mathbb{Z} \,\}, & \text{if } D \equiv 1 \pmod 4. \end{cases}$$

First we claim that $\mathcal{O}_K \supset R$. The minimal polynomial of $\sqrt{D}$ is $f(x) = x^2 - D \in \mathbb{Z}[x]$, so $\sqrt{D} \in \mathcal{O}_K$, implying that $\mathbb{Z}[\sqrt{D}] \subset \mathcal{O}_K$. (Regardless of whether D is congruent to 1 modulo 4 or not, as it happens).

If $D \equiv 1 \pmod 4$, then

$$f(x) = \Big(x - \frac{1+\sqrt{D}}{2}\Big)\Big(x - \frac{1-\sqrt{D}}{2}\Big) = x^2 - x + \frac{D-1}{4} \in \mathbb{Z}[x]$$

since $D-1$ is a multiple of 4, implying that $(1+\sqrt{D})/2 \in \mathcal{O}_K$, and so $\mathbb{Z}[\frac{1-\sqrt{D}}{2}] \subset \mathcal{O}_K$.

Secondly we show that $R \supset \mathcal{O}_K$. Suppose $\alpha = s + t\sqrt{D} \in \mathcal{O}_K$, with $s, t \in \mathbb{Q}$.

If $t = 0$, $\alpha = s \in \mathbb{Q} \cap \mathcal{O}_K = \mathbb{Z}$ implying, by the previous theorem, that $\alpha \in \mathbb{Z} \subset R$.

Hence assume $t \neq 0$. Then $\alpha \in \mathcal{O}_K$ if and only if the minimal polynomial of α over $\mathbb{Q}$, namely

$$p_\alpha(x) = (x - (s + t\sqrt{D}))(x - (s - t\sqrt{D})) = x^2 + 2sx + s^2 - t^2D$$

is in $\mathbb{Z}[x]$. This in turn is equivalent with $2s \in \mathbb{Z}$ and $s^2 - t^2D \in \mathbb{Z}$. Hence set $s' = 2s$, or $s = s'/2$.

We have two possibilities: s' is either even or odd.

Suppose s' is even. Then $s \in \mathbb{Z}$, so $t^2D \in \mathbb{Z}$ which, since D is square-free, means $t \in \mathbb{Z}$. Thus $\alpha = s + t\sqrt{D} \in R$ since $s, t \in \mathbb{Z}$, so $\mathcal{O}_K \subset R$.

Next suppose s' is odd. Let $n = s^2 - t^2D \in \mathbb{Z}$, which we rewrite as $n = (s'/2)^2 - t^2D$, or

$$4n = (s')^2 - (2t)^2D$$

meaning that $(2t)^2D \in \mathbb{Z}$ which, again by D being square-free, means $2t \in \mathbb{Z}$. Set $t' = 2t \in \mathbb{Z}$. Then $4n = (s')^2 - (t')^2D$. Reducing this modulo 4 we get $0 \equiv 1 - (t')^2D \pmod 4$ since s' is odd, so $(t')^2D \equiv 1 \pmod 4$. Now $(t')^2$ is either 0 or 1 modulo 4, but we can't have it being 0 since the product is 1, so $(t')^2 \equiv 1 \pmod 4$, and $D \equiv 1 \pmod 4$.

Hence t' is odd, and we learned along the way that this second case, with s' being odd, never happens if $D \not\equiv 1 \pmod 4$.

Now $D \equiv 1 \pmod 4$ means

$$\alpha = s + t\sqrt{D} = \frac{s'}{2} + \frac{t'}{2}\sqrt{D} = \underbrace{\frac{s' - t'}{2}}_{\in\mathbb{Z}} + t'\Big(\frac{1 + \sqrt{D}}{2}\Big) \in R$$

since s' and t' are both odd. □

2.2 The Cyclotomic Fields

We learned last time that it suffices to consider $K = \mathbb{Q}(\xi_m)$ with m even, since $\mathbb{Q}(\xi_m) = \mathbb{Q}(\xi_{2m})$ if m is odd. There are two things we aspire to show: first, that $\mathbb{Q}(\xi_m)$ are all distinct for even m, and secondly that $\mathcal{O}_K = \mathbb{Z}[\xi_m]$.

We'll recall some basic properties we'll need. Let $\omega = e^{2\pi i/m}$.

1. A ***(Galois) conjugate*** of ω is a root of a minimal polynomial of ω over $\mathbb{Q}$. Note that this has coefficients in $\mathbb{Z}$ since ω is an algebraic integer.

2. Every conjugate of ω is a primitive mth root of unity, i.e. a root of $x^m - 1$ but not a root of $x^n - 1$ for $n < m$.

3. The conjugates are ω^k for $1 \leq k \leq m$, $\gcd(k, m) = 1$.

Let ξ_m be a primitive mth root of unity and let $K = \mathbb{Q}(\xi_m)$. Then

4. $\deg(K/\mathbb{Q}) = \varphi(m)$,

5. $\mathrm{Gal}(K/\mathbb{Q}) \cong (\mathbb{Z}/m\mathbb{Z})^\times$.

Proposition 2.2.1. *If m is even, then the only roots of unity in $\mathbb{Q}(\xi_m)$ are mth roots of unity. In other words, $\theta \in \mathbb{Q}(\xi_m)$ with $\theta^n = 1$ implies $\theta^m = 1$.*

In addition, if m is off, then the only roots of unity in $\mathbb{Q}(\xi_m)$ are $(2m)$th roots of unity.

Proof. The second result follows immediately from the first since $\mathbb{Q}(\xi_m) = \mathbb{Q}(\xi_{2m})$ for m odd.

Hence assume m is even. Let $\theta \in \mathbb{Q}(\xi_m)$ be a primitive kth root of unity. Then $\mathbb{Q}(\xi_m)$ contains a primitive rth root of unity where $r = \operatorname{lcm}(k, m)$, since if $\theta = e^{2\pi i/k}$ and $\xi_m = e^{2\pi i/m}$ and $\gcd(k, m) = d = ak + bm$, we have

$$\xi_r = \theta^b \xi_m^a = e^{2\pi i(\frac{b}{k} + \frac{a}{m})} = e^{2\pi i \frac{bm+ak}{mk}} = e^{2\pi i \frac{d}{mk}} = e^{2\pi i/\operatorname{lcm}(m,k)} = e^{2\pi i/r}.$$

Now $\varphi(r) \mid \varphi(m)$. However $m \mid r$, meaning that $m = r$ so $k \mid m$. □

Corollary 2.2.2. *Let m be even. Then the mth cyclotomic fields $\mathbb{Q}(\xi_m)$ are all distinct.*

In order to prove $\mathcal{O}_K = \mathbb{Z}[\xi_m]$, we first need to discuss embeddings in $\mathbb{C}$.

2.3 Embeddings in $\mathbb{C}$

Let $K = \mathbb{Q}(\alpha)$ be a number field of degree n, meaning that α has n conjugates (since its minimal polynomial is of degree n). Each conjugate of β determines a unique embedding of K in $\mathbb{C}$, namely $\sigma\colon K \to \mathbb{C}$, $\alpha \mapsto \beta$. Hence there are exactly n embeddings of K in $\mathbb{C}$.

Example 2.3.1. Let $K = \mathbb{Q}(\sqrt{D})$ with D square-free. Then $\sqrt{D}$ has two conjugates, namely $\sqrt{D}$ itself and $-\sqrt{D}$. So we have two embeddings, $\sigma_1\colon K \to \mathbb{C}$ by $\sqrt{D} \mapsto \sqrt{D}$, namely the identity map, and $\sigma_2\colon K \mapsto \mathbb{C}$ by $\sqrt{D} \mapsto -\sqrt{D}$. Since both of the embeddings are contained in K, this is a Galois extension. ▲

Example 2.3.2. Let $K = \mathbb{Q}(\sqrt[3]{2})$. Since the minimal polynomial of $\sqrt[3]{2}$ over $\mathbb{Q}$ is $x^3 - 2$, there are three conjugates, and we can see them all by factoring this polynomial over $\mathbb{C}$. We get $\sqrt[3]{2}$, $\sqrt[3]{2}\omega$, and $\sqrt[3]{2}\omega^2$, where $\omega = (-1 + \sqrt{-3})/2$. Hence we have three embeddings, $\sigma_1, \sigma_2, \sigma_3\colon K \to \mathbb{C}$ by $\sqrt[3]{2} \mapsto \sqrt[3]{2}$, $\sqrt[3]{2} \mapsto \sqrt[3]{2}\omega$, and $\sqrt[3]{2} \mapsto \sqrt[3]{2}\omega^2$ respectively.

This extension is *not* Galois since $\sqrt[3]{2}\omega$ and $\sqrt[3]{2}\omega^2$ are not in K. ▲

More generally, if

$$\begin{array}{c} K \\ \big| m \\ L \\ \big| n \\ \mathbb{Q} \end{array}$$

meaning that K and L are number fields, then every embedding $\sigma\colon L \to \mathbb{C}$ can be extended to m embeddings of K in $\mathbb{C}$. In particular K has m embeddings in $\mathbb{C}$ that fix L pointwise.

Lecture 3 Traces, Norms, and Discriminants

3.1 Traces and Norms

Let K be a number field of degree n, and let $\sigma_1, \sigma_2, \ldots, \sigma_n$ be the embeddings of K in $\mathbb{C}$.

Definition 3.1.1. If $\sigma_i(K) \subset \mathbb{R}$, then σ_i is called a ***real embedding***. Otherwise σ_i is called a ***complex embedding***.

Fact. *The complex embeddings come in pairs. Since $\overline{\sigma}(x) \coloneqq \overline{\sigma(x)}$ is also a complex embedding of K in $\mathbb{C}$.*

Letting r_1 denote the number of real embeddings and r_2 denote the number of conjugate pairs of complex embeddings, we of course have $n = r_1 + 2r_2$.

Definition 3.1.2 (Trace and norm)**.** For any $\alpha \in K$, we define the ***trace*** of α to be

$$\mathrm{Tr}_{K/\mathbb{Q}}(\alpha) = \sigma_1(\alpha) + \sigma_2(\alpha) + \ldots + \sigma_n(\alpha)$$

and the ***norm*** of α to be

$$\mathrm{N}_{K/\mathbb{Q}}(\alpha) = \sigma_1(\alpha)\sigma_2(\alpha) \cdot \ldots \cdot \sigma_n(\alpha).$$

When it is obvious from context what field K we are working over we will omit the subscript $K/\mathbb{Q}$.

Exercise 3.1.3. Consider the $\mathbb{Q}$-linear map $L_\alpha \colon K \to K$ defined by $L_\alpha(x) = \alpha x$. Then $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha) = \mathrm{tr}(L_\alpha)$ and $\mathrm{N}_{K/\mathbb{Q}}(\alpha) = \det(L_\alpha)$.

The trace and norm behave largely as expected:

1. $\mathrm{Tr}(\alpha + \beta) = \mathrm{Tr}(\alpha) + \mathrm{Tr}(\beta)$,
2. If $r \in \mathbb{Q}$, then $\mathrm{Tr}(r\alpha) = r\,\mathrm{Tr}(\alpha)$ and $\mathrm{Tr}(r) = nr$,
3. $\mathrm{N}(\alpha\beta) = \mathrm{N}(\alpha)\,\mathrm{N}(\beta)$, and
4. If $r \in \mathbb{Q}$, then $\mathrm{N}(r\alpha) = r^n\,\mathrm{N}(\alpha)$ and $\mathrm{N}(r) = r^n$.

Theorem 3.1.4. *Let K be a number field of degree n and let $\alpha \in K$. Then*

$$\mathrm{Tr}_{K/\mathbb{Q}}(\alpha) = \frac{n}{d}\,\mathrm{Tr}_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\alpha)$$

and

$$\mathrm{N}_{K/\mathbb{Q}}(\alpha) = \big(\mathrm{N}_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\alpha)\big)^{n/d}$$

where $d = [\mathbb{Q}(\alpha) : \mathbb{Q}]$, meaning that $d \mid n$.

Proof. There exist d embeddings of $\mathbb{Q}(\alpha)$ in $\mathbb{C}$, say $\sigma_1, \sigma_2, \ldots, \sigma_d$. Each σ_i extends to exactly n/d embeddings of K in $\mathbb{C}$, say $\sigma_{i,1}, \sigma_{i,2}, \ldots, \sigma_{i,n/d}$. Then

$$\{\,\sigma_{i,j}\,\}_{\substack{1 \le i \le d \\ 1 \le j \le n/d}}$$

Date: January 16th, 2018.

gives all n embeddings of K in $\mathbb{C}$. Hence

$$\mathrm{Tr}_{K/\mathbb{Q}}(\alpha) = \sum_{i,j} \sigma_{i,j}(\alpha) = \sum_i \frac{n}{d}\sigma_i(\alpha) = \frac{n}{d}\,\mathrm{Tr}_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\alpha)$$

since for $\alpha \in K$ we have $\sigma_{i,j}(\alpha) = \sigma_i(\alpha)$ for all j.

Similarly

$$\mathrm{N}_{K/\mathbb{Q}}(\alpha) = \prod_{i,j} \sigma_{i,j}(\alpha) = \prod_i (\sigma_i(\alpha))^{n/d} = \Big(\mathrm{N}_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\alpha)\Big)^{n/d}. \qquad \square$$

Corollary 3.1.5. *For $\alpha \in K$ we have*

$$\mathrm{Tr}_{K/Q}(\alpha), \mathrm{N}_{K/Q}(\alpha) \in \mathbb{Q}$$

and if $\alpha \in \mathcal{O}_K$ we have

$$\mathrm{Tr}_{K/Q}(\alpha), \mathrm{N}_{K/Q}(\alpha) \in \mathbb{Z}.$$

Proof. Let $p_\alpha(x) = x^d + a_{d-1}x^{d-1} + \ldots + a_1 x + a_0$ be the monic minimal polynomial of α over $\mathbb{Q}$. Then we know moreover that

$$p_\alpha(x) = (x - \sigma_1(\alpha))(x - \sigma_2(\alpha)) \cdot \ldots \cdot (x - \sigma_d(\alpha))$$

since $\sigma_i(\alpha)$ are the Galois conjugates of α. Hence, multiplying out,

$$\mathrm{Tr}_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\alpha) = -a_{d-1} \in \mathbb{Q}$$

and

$$\mathrm{N}_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\alpha) = \pm a_0 \in \mathbb{Q}$$

(with the plus or minus depending on the degree d). By Theorem 3.1.4 we therefore moreover have $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha)$ and $\mathrm{N}_{K/\mathbb{Q}}(\alpha)$ in $\mathbb{Q}$, since they are rationals times integers.

If $\alpha \in \mathcal{O}_K$, then $a_i \in \mathbb{Z}$ by definition, whence the above become the products of integers, hence integers. $\square$

Note that

$$\mathrm{Tr}_{K/\mathbb{Q}} \colon K \to (\mathbb{Q}, +)$$

is an additive homomorphism and that

$$\mathbb{N}_{K/\mathbb{Q}} \colon K^* \to (\mathbb{Q}, \cdot)$$

is a multiplicative homomorphism, whereby K^* we mean $K \setminus \{\,0\,\}$.

Example 3.1.6. Let $K = \mathbb{Q}(\sqrt{D})$ with D square-free, and let $\alpha = a + b\sqrt{D}$ with $a, b \in \mathbb{Q}$. Then

$$\mathrm{Tr}(\alpha) = (a + b\sqrt{D}) + (a - b\sqrt{D}) = 2a$$

and

$$\mathrm{N}(\alpha) = (a + b\sqrt{D})(a - b\sqrt{D}) = a^2 - b^2 D. \qquad \blacktriangle$$

These constructs are not just idle curiosities. Indeed, computing norms can offer insight into whether something is a unit.

Let $\alpha \in \mathcal{O}_K$ be a unit. Then $\mathrm{N}(\alpha) = \pm 1$. Seeing this is easy: $\alpha, \alpha^{-1} \in \mathcal{O}_K$ implies $\mathrm{N}(\alpha\alpha^{-1}) = \mathrm{N}(1) = 1$, meaning that $\mathrm{N}(\alpha)\,\mathrm{N}(\alpha^{-1}) = 1$, so $\mathrm{N}(\alpha) \mid 1$.

Another observation: let $\alpha \in OO_K$ so that $N(\alpha) \in \mathbb{Z}$ is a prime. Then α is irreducible, since $\alpha = \beta_1\beta_2$ is equivalent with $\mathrm{N}(\alpha) = \mathrm{N}(\beta_1)\,\mathrm{N}(\beta_2)$, so if the left-hand side is a prime, one of the elements in the right-hand side must be a unit.

Example 3.1.7. This tells us that, for instance, $\mathbb{Z}[\sqrt{-2}]^\times = \{1, -1\}$ since $\mathrm{N}(\alpha) = a^2 + 2b^2 = 1$, forcing $b = 0$, and hence $a = \pm 1$.

It also tells us that, say, $9 + \sqrt{10}$ is irreducible in $\mathbb{Z}[\sqrt{10}]$ since $\mathrm{N}(9 + \sqrt{10}) = 71$, which is prime. ▲

3.2 Relative Trace and Norm

We don't necessarily have to consider traces and norms with respect to $\mathbb{Q}$.

Definition 3.2.1 (Relative trace and norm)**.** Let K and L be two number fields such that $K \subset L$ and $[L : K] = n$. Let $\sigma_1, \sigma_2, \ldots, \sigma_n$ be the n embeddings of L in $\mathbb{C}$ that fix K. For all $\alpha \in L$ we define the ***relative trace***

$$\mathrm{Tr}_{L/K}(\alpha) = \sigma_1(\alpha) + \sigma_2(\alpha) + \ldots + \sigma_n(\alpha)$$

and ***relative norm*** by

$$\mathrm{N}_{L/K}(\alpha)\sigma_1(\alpha)\sigma_2(\alpha) \cdot \ldots \cdot \sigma_n(\alpha).$$

As before, these are homomorphisms, and if $\alpha \in \mathcal{O}_L$, then $\mathrm{Tr}_{L/K}(\alpha) \in \mathcal{O}_K$.

Theorem 3.2.2 (Transitivity)**.** *Let K, L, and M be number fields with $K \subset L \subset M$. Then for $\alpha \in M$ we have*

$$\mathrm{Tr}_{L/K}(\mathrm{Tr}_{M/L}(\alpha)) = \mathrm{Tr}_{M/K}(\alpha)$$

along with

$$\mathrm{N}_{L/K}(\mathrm{N}_{M/L}(\alpha)) = \mathrm{N}_{M/K}(\alpha).$$

Proof. Let $[M : L] = m$ and $[L : K] = n$, and let $\tau_1, \tau_2, \ldots, \tau_m$ be the embeddings of M in $\mathbb{C}$ which fix L, and $\sigma_1, \sigma_2, \ldots, \sigma_n$ be the embeddings of L in $\mathbb{C}$ which fix K.

Take N to be a normal extension of $\mathbb{Q}$ such that $N \supset M$. The extension being normal means that every embedding can be extended to it, whereby we let $\bar{\tau}_i$ be the extension of τ_i to N and $\bar{\sigma}_j$ the extension of σ_j to N. In other words they are automorphisms from N to N.

Then we have

$$\mathrm{Tr}_{L/K}(\mathrm{Tr}_{M/K}(\alpha)) = \mathrm{Tr}_{L/K}\left(\sum_i \tau_i(\alpha)\right) = \sum_j \sum_i \sigma_j(\tau_i(\alpha)) = \sum_j \sum_i \bar{\sigma}_j(\bar{\tau}_i(\alpha))$$

(where we brought the inner sum outside since these are homomorphisms). We now need to show that this is the same as $\mathrm{Tr}_{M/K}(\alpha)$.

Now we know by degree considerations that there are nm embeddings of M in $\mathbb{C}$ that fix K, so if we can show that

$$\{\,\bar{\sigma}_j\bar{\tau}_i\,\}_{\substack{1\le i\le m\\ 1\le j\le n}}$$

are all distinct, then they must be the mn embeddings of M in $\mathbb{C}$ that fix K.

Suppose therefore that $\bar{\sigma}_{j_1}\bar{\tau}_{i_1} = \bar{\sigma}_{j_2}\bar{\tau}_{i_2}$ on M. For $x \in L$,

$$\bar{\sigma}_{j_1}(\bar{\tau}_{i_1}(x)) = \bar{\sigma}_{j_1}(\tau_{i_1}(x)) = \bar{\sigma}_{j_1}(x)$$

and

$$\bar{\sigma}_{j_2}(\bar{\tau}_{i_2}(x)) = \bar{\sigma}_{j_2}(\tau_{i_2}(x)) = \bar{\sigma}_{j_2}(x)$$

since in L, $\bar{\tau}_i(x) = \tau_i(x) = x$. Moreover these two remain equal, so $\bar{\sigma}_{j_1}(x) = \bar{\sigma}_{j_2}(x)$ for all $x \in L$. By the same argument again therefore this means $\sigma_{j_1}(x) = \sigma_{j_2}(x)$, so $j_1 = j_2$, whence $\bar{\tau}_{i_1} = \bar{\tau}_{i_2}$ on M, so $i_1 = i_2$.

The argument for the norm is almost identical, but with products in place of sums. □

3.3 Discriminants

Definition 3.3.1 (Discriminant)**.** Let K be a number field of degree n and let $\sigma_1, \sigma_2, \ldots, \sigma_n$ be the n embeddings of K in $\mathbb{C}$. For any n elements

$$\alpha_1, \alpha_2, \ldots, \alpha_n \in K,$$

we define the ***discriminant*** of $\alpha_1, \alpha_2, \ldots, \alpha_n$ by

$$\operatorname{disc}(\alpha_1, \alpha_2, \ldots, \alpha_n) = \Big(\det[\sigma_i(\alpha_j)]_{\substack{1\le i\le n\\ 1\le j\le n}}\Big)^2.$$

Note that because of the square the discriminant is independent of the order of embeddings or elements, since permuting these simply changes the sign, but squaring nullifies this.

Theorem 3.3.2. *With the setup as in the definition above, we have*

$$\operatorname{disc}(\alpha_1, \alpha_2, \ldots, \alpha_n) = \det([\operatorname{Tr}_{K/\mathbb{Q}}(\alpha_i\alpha_j)]).$$

Proof. Note that

$$\det([\operatorname{Tr}_{K/\mathbb{Q}}(\alpha_i\alpha_j)]) = [\sigma_j(\alpha_i)][\sigma_i(\alpha_j)]$$

where the two matrices in the right-hand side are each others transposes. Taking determinants now we get the expression sought. □

Corollary 3.3.3. *Again with the setup as above, we have* $\operatorname{disc}(\alpha_1, \alpha_2, \ldots, \alpha_n) \in \mathbb{Q}$ *and if* $\alpha_i \in \mathcal{O}_K$*, then* $\operatorname{disc}(\alpha_1, \alpha_2, \ldots, \alpha_n) \in \mathbb{Z}$.

Lecture 4 The Additive Structure of the Ring of Integers

4.1 More on Discriminants

Theorem 4.1.1. *With the same setup as above,* $\operatorname{disc}(\alpha_1, \alpha_2, \ldots, \alpha_n) = 0$ *if and only if* $\alpha_1, \alpha_2, \ldots, \alpha_n$ *are linearly dependent over* $\mathbb{Q}$.

Proof. We start by assuming $\alpha_1, \alpha_2, \ldots, \alpha_n$ are linearly dependent over $\mathbb{Q}$. This means that $[\sigma_i(\alpha_j)]$ has linearly dependent column vectors over $\mathbb{Q}$, whence its determinant is 0, and so the discriminant is 0 too.

For the converse, assume $\operatorname{disc}(\alpha_1, \alpha_2, \ldots, \alpha_n) = 0$. This means that the matrix $[\operatorname{Tr}(\alpha_i \alpha_j)]$ has linearly dependent row vectors.

Let R_i be the ith row vector of this matrix. Then

$$a_1 R_1 + a_2 R_2 + \ldots + a_n R_n = 0 \tag{4.1.1}$$

for some $a_i \in \mathbb{Q}$ with not all $a_i = 0$. Let

$$\alpha = a_1 \alpha_1 + a_2 \alpha_2 + \ldots + a_n \alpha_n.$$

The jth coordinate of (4.1.1) is

$$a_1 \operatorname{Tr}(\alpha_1 \alpha_j) + a_2 \operatorname{Tr}(\alpha_2 \alpha_j) + \ldots + a_n \operatorname{Tr}(\alpha_n \alpha_j) = 0$$

which by linearity of trace we can rewrite as

$$\operatorname{Tr}((a_1 \alpha_1 + a_2 \alpha_2 + \ldots + a_n \alpha_n)\alpha_j) = 0$$

and so in all

$$\operatorname{Tr}(\alpha \alpha_j) = 0$$

for all j.

Now suppose $\alpha_1, \alpha_2, \ldots, \alpha_n$ are linearly independent over $\mathbb{Q}$, meaning that they form a basis for K over $\mathbb{Q}$ and $\alpha \neq 0$ implies $\alpha\alpha_1, \alpha\alpha_2, \ldots, \alpha\alpha_n$ is also a basis for K over $\mathbb{Q}$.

But the last equation above then means that Tr is 0 on a basis, whence $\operatorname{Tr}(x) = 0$ for all $x \in K$. This is a contradiction, since we know $\operatorname{Tr}(1) = n \neq 0$. □

We get a special case of the discriminant if we select $\alpha_1, \alpha_2, \ldots, \alpha_n$ to be powers of α:

Proposition 4.1.2. *Let* $K = \mathbb{Q}(\alpha)$ *with* $[K : \mathbb{Q}] = n$. *Then* $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ *is a basis for* K *over* $\mathbb{Q}$, *and*

$$\begin{aligned} \operatorname{disc}(\alpha) \coloneqq \operatorname{disc}(1, \alpha, \alpha^2, \ldots, \alpha^{n-1}) &= \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)^2 \\ &= (-1)^{n(n-1)/2} \operatorname{N}_{K/\mathbb{Q}}(f'(\alpha)) \end{aligned}$$

where $f(x) = \prod_{i=1}^{n} (x - \alpha_i)$ *is the monic minimal polynomial of* α *over* $\mathbb{Q}$, *with* $\alpha_i = \sigma_i(\alpha)$.

Date: January 18th, 2018.

Proof. We have

$$\operatorname{disc}(\alpha) = \det([\sigma_i(\alpha^j)])^2 = \det([\alpha_i^j])^2$$

which is a Vandermode matrix, so this is equal to

$$\begin{aligned}\prod_{1\le i<j\le n}(\alpha_i-\alpha_j)^2 &= \Big(\prod_{1\le i<j\le n}(\alpha_i-\alpha_j)\Big)^2 = (-1)^{n(n-1)/2}\prod_i\prod_{j\neq i}(\alpha_i-\alpha_j)\\ &= (-1)^{n(n-1)/2}\prod_i f'(\alpha_i) = (-1)^{n(n-1)/2}\,\mathrm{N}_{K/\mathbb{Q}}(f'(\alpha))\end{aligned}$$

by the product rule and counting how many minus signs there are. The shift from product of $f'(\alpha_i)$ to the norm is seeing $\alpha_i = \sigma_i(\alpha)$ and using the fact that σ_i is a homomorphism to factor it. □

Example 4.1.3. Let $K = \mathbb{Q}(\xi_p)$ with $\xi_p = e^{2\pi i/p}$ and p a prime. Say $p \ge 3$, since otherwise $K = \mathbb{Q}$. Then $[K:\mathbb{Q}] = \varphi(p) = p-1$, whence we consider

$$\operatorname{disc}(\xi_p) = \operatorname{disc}(1, \xi_p, \ldots, \xi_p^{p-2}).$$

The monic minimal polynomial of ξ_p over $\mathbb{Q}$ is

$$f(x) = x^{p-1} + x^{p-2} + \ldots + x + 1$$

and we would like to compute $f'(\xi_p)$ and in particular $\mathrm{N}_{K/\mathbb{Q}}(f'(\xi_p))$. Rather than doing this directly, note that $x^p - 1 = (x-1)f(x)$, so by the product rule

$$px^{p-1} = f(x) + (x-1)f'(x)$$

whereby if we plug in $x = \xi_p$ we have

$$p\xi_p^{p-1} = (\xi - 1)f'(\xi_p)$$

which we rearrange to

$$f'(\xi_p) = \frac{p\xi_p^{p-1}}{\xi_p - 1}.$$

Taking norms and recalling that it is a multiplicative homomorphism, we get

$$\mathrm{N}(f'(\xi_p)) = \frac{\mathrm{N}(p)\,\mathrm{N}(\xi_p)^{p-1}}{\mathrm{N}(\xi_p - 1)}.$$

We evaluate the factors of the right-hand side one at a time. First, $\mathrm{N}(p) = p^{p-1}$. Next $\mathrm{N}(\xi_p)$ by definition is the product of then conjugates of ξ_p, so

$$\mathrm{N}(\xi_p) = \xi_p\xi_p^2 \cdot \ldots \cdot \xi_p^{p-1} = \xi_p^{p(p-1)/2} = (\xi_p^p)^{(p-1)/2} = 1.$$

Finally

$$f(x) = x^{p-1} + x^{p-2} + \ldots + x + 1 = (x-\xi_p)(x-\xi_p^2)\cdot \ldots \cdot (x-\xi_p^{p-1})$$

whereby

$$f(1) = p = (1-\xi_p)(1-\xi_p^2)\cdot \ldots \cdot (1-\xi_p^{p-1}) = \mathrm{N}(1-\xi_p) = \mathrm{N}(\xi_p - 1).$$

Hence

$$\mathrm{N}(f'(\xi_p)) = \frac{p^{p-1} \cdot 1}{p} = p^{p-2},$$

whereby

$$\mathrm{disc}(\xi_p) = (-1)^{p(p-1)/2} p^{p-2},$$

meaning that $\mathrm{disc}(\xi_p) \mid p^{p-2}$. ▲

Something more general is true:

Example 4.1.4. Let $K = \mathbb{Q}(\xi_m)$, with $\xi_m = e^{2\pi i/m}$. Then $\mathrm{disc}(\xi_m) \mid m^{\varphi(m)}$.

Let $f(x)$ be the monic minimal polynomial of ξ_m over $\mathbb{Q}$ again. Then $x^m - 1 = f(x)g(x)$, wherein $f(x), g(x) \in \mathbb{Z}[x]$ by Gauss lemma. Therefore again by the product rule

$$mx^{m-1} = f'(x)g(x) + f(x)g'(x)$$

whence $m\xi_m^{m-1} = f'(\xi_m)g(\xi_m)$, since ξ_m is a root of $f(x)$ itself. Multiplying both sides by ξ_m we get

$$m = \xi_m f'(\xi_m)g(\xi_m)$$

which if we take norms becomes

$$m^{\varphi(m)} = \mathrm{N}(f'(\xi_m))\,\mathrm{N}(g(\xi_m)\xi_m)$$

wherein $g(\xi_m)\xi_m \in \mathcal{O}_K$ so the second norm is in $\mathbb{Z}$. The same is true for the first one, in both cases since ξ_m is an algebraic integer. Hence $\mathrm{disc}(\xi_m) \mid m^{\varphi(m)}$, since note that the first norm is $\mathrm{disc}(\xi_m)$ save for maybe a sign. ▲

4.2 The Additive Structure of the Ring of Integers

As per usual, let K be a number field of degree n. The goal now is to show that $\mathcal{O}_K$ is a free abelian group of rank n (or in other words a free $\mathbb{Z}$-module of rank n).

First recall some facts about such matters:

Fact. *A free abelian group of finite rank n is isomorphic to*

$$\mathbb{Z} \oplus \mathbb{Z} \oplus \ldots \oplus \mathbb{Z} = \mathbb{Z}^n.$$

Fact. *Every subgroup of a free abelian group of rank n is also a free abelian group of rank $m \leq n$.*

For an example that doesn't decrease the rank, consider for instance replacing one of the $\mathbb{Z}$'s above with $2\mathbb{Z}$.

Corollary 4.2.1. *Let $G_1 \subset G_2 \subset G_3$ be groups. If G_1 and G_3 are free abelian groups of rank n, then so is G_2.*

Hence our strategy is to show that $\mathcal{O}_K$ is between two free abelian groups of rank n.

Remark 4.2.2. We know that K has a basis $\alpha_1, \alpha_2, \ldots, \alpha_n$ over $\mathbb{Q}$. In fact, we can arrange for this basis to be elements from $\mathcal{O}_K$, since any $\alpha_i = \beta_i/m_i$ with $\beta_i \in \mathcal{O}_K$ and $m_i \in \mathbb{Z}$, so scaling to get rid of the denominator yields a basis in $\mathcal{O}_K$.

Hence $K = \mathbb{Q}(\alpha)$, and we can assume $\alpha \in \mathcal{O}_K$, and the basis is

$$1, \alpha, \ldots, \alpha^{n-1}.$$

Notice now that $K \supset \mathcal{O}_K \supsetneq \mathbb{Z}[\alpha]$. The latter is a free abelian group of rank n though, so half of our inclusion is trivially true.

Letting $\alpha_1, \alpha_2, \ldots, \alpha_n$ be a basis contained in $\mathcal{O}_K$, consider

$$G = \mathbb{Z}\alpha_1 \oplus \mathbb{Z}\alpha_2 \oplus \ldots \oplus \mathbb{Z}\alpha_n = \{\, m_1\alpha_1 + m_2\alpha_2 + \ldots + m_n\alpha_n \mid m_i \in \mathbb{Q} \,\}.$$

This is a free abelian group of rank n on $\alpha_1, \alpha_2, \ldots, \alpha_n$.

We claim, and soon prove, that

$$G \subset \mathcal{O}_K \subset \frac{1}{d}G = \mathbb{Z}\frac{\alpha_1}{d} \oplus \mathbb{Z}\frac{\alpha_2}{d} \oplus \ldots \oplus \mathbb{Z}\frac{\alpha_n}{d},$$

where $d = \operatorname{disc}(\alpha_1, \alpha_2, \ldots, \alpha_n)$.

Theorem 4.2.3. *Let $d = \operatorname{disc}(\alpha_1, \alpha_2, \ldots, \alpha_n)$. Then $\mathcal{O}_K \subset \frac{1}{d}G$. In fact, every $\alpha \in \mathcal{O}_K$ can be written as*

$$\alpha = \frac{m_1\alpha_1 + m_2\alpha_2 + \ldots + m_n\alpha_n}{d}$$

with $m_i \in \mathbb{Z}$ and $d \mid m_i^2$.

Before we prove this, note two things: $d \neq 0$ since α_i is a basis, and $d \in \mathbb{Z}$ since $\alpha_i \in \mathcal{O}_K$.

Note also that this being true, we have the immediate corollary we want:

Corollary 4.2.4. *Let K be a number field of degree n. Then $\mathcal{O}_K$ is a free abelian group of rank n.*

Proof of theorem. Let $\alpha \in \mathcal{O}_K$, whereby $\alpha = x_1\alpha_1 + x_2\alpha_2 + \ldots + x_n\alpha_n$ for some $x_i \in \mathbb{Q}$ with α_i forming a basis. Moreover let $\sigma_1, \sigma_2, \ldots, \sigma_n$ be the embeddings of K in $\mathbb{C}$.

Then we have the following system of equations

$$\begin{cases} \sigma_1(\alpha_1)x_1 + \sigma_1(\alpha_2)x_2 + \ldots + \sigma_1(\alpha_n)x_n = \sigma_1(\alpha) \\ \sigma_2(\alpha_1)x_1 + \sigma_2(\alpha_2)x_2 + \ldots + \sigma_2(\alpha_n)x_n = \sigma_2(\alpha) \\ \quad\vdots \\ \sigma_n(\alpha_1)x_1 + \sigma_n(\alpha_2)x_2 + \ldots + \sigma_n(\alpha_n)x_n = \sigma_n(\alpha) \end{cases}$$

which we rewrite as

$$\big[\sigma_i(\alpha_j)\big] \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} \sigma_1(\alpha) \\ \sigma_2(\alpha) \\ \vdots \\ \sigma_n(\alpha) \end{bmatrix}.$$

If we solve for x_i using Cramer's rule, letting $\delta = \det([\sigma_i(\alpha_j)])$, whence $\delta^2 = d \in \mathbb{Z}$, we have $x_i = \gamma_i/\delta$, where σ_i is the determinant of the original matrix $[\sigma_i(\alpha_j)]$ except with the ith column replaced by the right-hand side of the system.

Hence $dx_i = \delta^2\gamma_i/\delta = \delta\gamma_i$. □

Lecture 5 Integral Bases

5.1 Integral Bases

We start by finishing the proof from last time.

Proof continued. We have $dx_i = \delta\gamma_i$, where since $d \in \mathbb{Z}$ and $x_i \in \mathbb{Q}$ the left-hand side is in $\mathbb{Q}$, and the right-hand side is an algebraic integer if $\alpha \in \mathcal{O}_K$, so indeed it is an integer. Then $dx_i = m_i \in \mathbb{Z}$, and we write $x_i = m_i/d$, whence

$$\alpha = \frac{m_1\alpha_1 + m_2\alpha_2 + \ldots + m_n\alpha_n}{d}.$$

Next we have

$$\frac{m_i^2}{d} = \frac{d^2x_i^2}{d} = dx_i^2 = \delta^2\frac{\gamma_i^2}{\delta^2} = \gamma_i^2,$$

which is an algebraic integer in $\mathbb{Q}$, so it's an integer. Hence $d \mid m_i^2$. □

Definition 5.1.1 (Integral basis)**.** Let K be a number field of dimension n. Since $\mathcal{O}_K$ has a basis over $\mathbb{Z}$ (since it's a free abelian group) there exists $\beta_1, \beta_2, \ldots, \beta_n \in \mathcal{O}_K$ such that every $\alpha \in \mathcal{O}_K$ can be written as

$$\alpha = m_1\beta_1 + m_2\beta_2 + \ldots + m_n\beta_n,$$

with $m_i \in \mathbb{Z}$. Such a basis $\{\beta_1, \beta_2, \ldots, \beta_n\}$ is called an ***integral basis*** for $\mathcal{O}_K$ (or K).

Note that if we take $m_i \in \mathbb{Q}$, the above will span K.

Example 5.1.2. Let $K = \mathbb{Q}(\sqrt{D})$, with D being square-free. Then $\mathcal{O}_K$ is $\mathbb{Z}[\sqrt{D}]$ if $D \not\equiv 1 \pmod 4$ and $\mathbb{Z}[(1+\sqrt{D})/2]$ if $D \equiv 1 \pmod 4$.

Hence $\mathcal{O}_K$ has the integral basis $\{1, \sqrt{D}\}$ in the former case and $\{1, (1+\sqrt{D})/2\}$ in the latter. ▲

Theorem 5.1.3. *Let $K = \mathbb{Q}(\xi_{p^r})$, with $\xi_{p^r} = e^{2\pi i/p^r}$ and $p^r \geq 3$ for p prime. Then $\mathcal{O}_K = \mathbb{Z}[\xi_{p^r}]$.*

We will need two lemmas to prove this.

Lemma 5.1.4. *With $\xi = \xi_{p^r}$ as above, $\mathbb{Z}[1-\xi] = \mathbb{Z}[\xi]$, and* $\operatorname{disc}(1-\xi) = \operatorname{disc}(\xi)$.

Proof. The first statement is clear: $\mathbb{Z}[\xi] \subset \mathbb{Z}[1-\xi]$ since $1-\xi \in \mathbb{Z}[\xi]$, and since $1-(1-\xi) = \xi$ the opposite inclusion is true as well.

For the second statement we have

$$\operatorname{disc}(\xi) = \prod_{1\leq i<j\leq n}(\alpha_i - \alpha_j)^2 = \prod_{1\leq i<j\leq n}((1-\alpha_i) - (1-\alpha_j))^2 = \operatorname{disc}(1-\xi)$$

since $1-\alpha_i$ are the Galois conjugates to $1-\xi$, calling α_i the conjugates to ξ itself. □

Date: January 23rd, 2018.

Lemma 5.1.5. *With the same setup,*

$$\prod_{\substack{1\le k\le p^r\\ p\nmid k}} (1-\xi^k) = p$$

meaning that $\mathrm{N}(1-\xi) = p$.

Proof. The monic minimal polynomial of ξ over $\mathbb{Q}$ is

$$f(x) = \prod_{\substack{1\le k\le p^r\\ p\nmid k}} (x-\xi^k) = \frac{x^{p^r}-1}{x^{p^{r-1}}-1} = \frac{t^p-1}{t-1} = t^{p-1}+t^{p-2}+\ldots+t+1$$

with $t = x^{p^{r-1}}$. Hence taking $x = 1$ gives $t = 1$ i.e.

$$f(1) = p = \prod_{\substack{1\le k\le p^r\\ p\nmid k}} (1-\xi^k). \qquad \square$$

We are now ready to prove the theorem:

Proof of theorem. Taking, again, $\xi = \xi_{p^r}$, we have $\{\,1,\xi,\xi^2,\ldots,\xi^{n-1}\,\} \subset \mathcal{O}_K$ with $n = \varphi(p^r)$ is a basis for K over $\mathbb{Q}$. So therefore is

$$\{\,1,(1-\xi),(1-\xi)^2,\ldots,(1-\xi)^{n-1}\,\} \subset \mathcal{O}_K.$$

Hence we can write $\alpha \in \mathcal{O}_K$ as

$$\alpha = \frac{m_1 + m_2(1-\xi)+\ldots+m_n(1-\xi)^{n-1}}{d},$$

where $d = \mathrm{disc}(1-\xi) = \mathrm{disc}(\xi)$ by the first lemma.

We now claim that $\mathcal{O}_K = \mathbb{Z}[1-\xi]$, which by the first lemma is the same as $\mathbb{Z}[\xi]$. Suppose $\mathcal{O}_K$ is strictly larger than $\mathbb{Z}[1-\xi]$, i.e. there exists some $\alpha \in \mathcal{O}_K$ such that $d \nmid m_i$ for some i. Note that $d \mid (p^r)^{\varphi(p^r)}$, so $d = p^r$ for some r. There must exist some element in $\mathcal{O}_K$ of the form

$$\beta = \frac{t_i(1-\xi)^{i-1}+\ldots+t_n(1-\xi)^{n-1}}{p}$$

with $t \nmid t_i$.

Hint. Let $m_{j_1},\cdots,m_{j_k}$ be all m_is that are not divisible by $d = p^r$. Write $m_{j_s} = p^{r_{j_s}}t_{j_s}$ with $(t_{j_s},p) = 1$ and $r_{j_s} < r$. Take i to be the smallest index such that $r_i = \min\{\,r_{j_s}\,\}$. Consider $p^{r-r_i-1}\alpha$ subtracting its first $(i-1)$ terms.

Note that $1-\xi \mid 1-\xi^k$ for all k, so $(1-\xi)^{\varphi(p^r)} = (1-\xi)^n \mid p$, meaning that $p/(1-\xi)^i \in \mathbb{Z}[\xi]$ for $1 \le i \le n$.

Therefore

$$\frac{p}{(1-\xi)^i}\beta = \frac{t^i}{1-\xi} + t_{i+1} + t_{i+2}(1-\xi)+\ldots+t_n(1-\xi)^{n-i-1},$$

where the sum of the latter terms are in $\mathbb{Z}[1-\xi] \subset \mathcal{O}_K$. This implies that $t_i/(1-\xi) \in \mathcal{O}_K$, whence

$$\mathrm{N}_{K/\mathbb{Q}}\left(\frac{t_i}{1-\xi}\right) \in \mathbb{Z}$$

so $t_i^n/\,\mathrm{N}(1-\xi) = t_i^n/p \in \mathbb{Z}$, meaning that $p \mid t_i$, which is a contradiction. Hence $\mathcal{O}_K = \mathbb{Z}[1-\xi] = \mathbb{Z}[\xi]$. $\square$

Theorem 5.1.6. *Let* $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ *and* $\{\beta_1, \beta_2, \ldots, \beta_n\}$ *be two integral bases for* $\mathcal{O}_K$. *Then* $\operatorname{disc}(\alpha_1, \alpha_2, \ldots, \alpha_n) = \operatorname{disc}(\beta_1, \beta_2, \ldots, \beta_n)$.

Proof. Express the α_i in terms of β_j's, say

$$\begin{bmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{bmatrix} = M \begin{bmatrix} \beta_1 \\ \beta_2 \\ \vdots \\ \beta_n \end{bmatrix}$$

where M is an $n \times n$ matrix with elements in $\mathbb{Z}$. Hence

$$\operatorname{disc}(\alpha_1, \alpha_2, \ldots, \alpha_n) = \det([\sigma_i(\alpha_j)])^2 = \det(M[\sigma_i(\beta_j)])^2 = \det(M)^2 \operatorname{disc}(\beta_1, \beta_2, \ldots, \beta_n)$$

whence $\operatorname{disc}(\beta_1, \beta_2, \ldots, \beta_n) \mid \operatorname{disc}(\alpha_1, \alpha_2, \ldots, \alpha_n)$ and by reversing the argument we have the opposite divisibility as well. Now since they both have the same sign, since $\det(M)^2 > 0$, they must be equal. □

Definition 5.1.7. Let K be a number field, and let $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ be an integral basis for $\mathcal{O}_K$. Define the ***discriminant*** of K (or $\mathcal{O}_K$) by

$$\operatorname{disc}(K) = \operatorname{disc}(\mathcal{O}_K) = \operatorname{disc}(\alpha_1, \alpha_2, \ldots, \alpha_n)$$

which by the above theorem is independent of the choice of integral basis.

Exercise 5.1.8. Consider $\{\alpha_1, \alpha_2, \ldots, \alpha_n\} \subset \mathcal{O}_K$. Then $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ is an integral basis for $\mathcal{O}_K$ if and only of $\operatorname{disc}(\alpha_1, \alpha_2, \ldots, \alpha_n) = \operatorname{disc}(K)$.

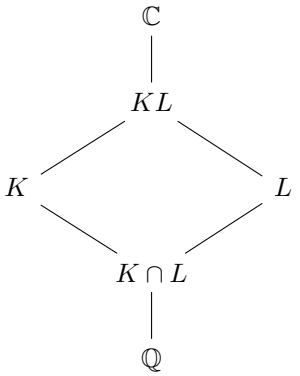
5.2 Composite Field

Definition 5.2.1 (Composite Field)**.** Let K be a number field of degree m and let L be a number field of degree n. Then

$$KL = \left\{ \sum_{i=1}^{r} \alpha_i \beta_i \;\middle|\; \alpha_i \in K, \beta_i \in L \right\}$$

is a subfield of $\mathbb{C}$ called the ***composition*** of K and L.

We have the following inclusions:



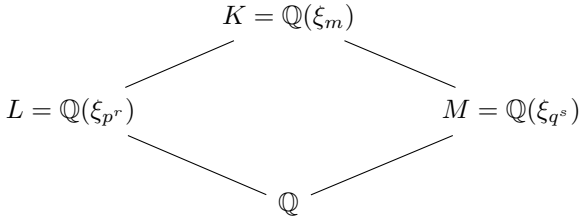
A few facts follow immediately from this definition:

- $[KL : K] \leq [L : L \cap K]$,
- $[KL : \mathbb{Q}] \leq [K : \mathbb{Q}] \cdot [L : \mathbb{Q}]$,
- Define
$$\mathcal{O}_K \cdot \mathcal{O}_L = \left\{ \sum_{i=1}^{r} \alpha_i \beta_i \;\middle|\; \alpha_i \in \mathcal{O}_K, \beta_i \in \mathcal{O}_L \right\}$$
then $\mathcal{O}_K \cdot \mathcal{O}_L \subset \mathcal{O}_{KL}$.

Lecture 6 Composition Fields

6.1 Cyclotomic Fields again

We are soon ready to prove what has been our goal for quite some time now, namely that if $K = \mathbb{Q}(\xi_m)$, then $\mathcal{O}_K = \mathbb{Z}[\xi_m]$. We know that this is true for $m = p^r$, so what about general m? The strategy is to prime factorise m, because if, say, $m = p^r q^s$ with p and q distinct primes, and $L = \mathbb{Q}(\xi_{p^r})$ and $M = \mathbb{Q}(\xi_{q^s})$, we have



and we will show that $K = LM$ and moreover $\mathcal{O}_K = \mathbb{Z}[\xi_{p^r}]\mathbb{Z}[\xi_{q^s}] = \mathbb{Z}[\xi_m]$.

Proposition 6.1.1. *Let K and L be two number fields with $[K : \mathbb{Q}] = m$ and $[L : \mathbb{Q}] = n$. Assume $[KL : \mathbb{Q}] = mn$, i.e. $K \cap L = \mathbb{Q}$, and let $d = \gcd(\operatorname{disc}(K), \operatorname{disc}(L))$. Then*

$$\mathcal{O}_{KL} \subset \frac{1}{d} \mathcal{O}_K \cdot \mathcal{O}_L.$$

An immediate result that follows is

Corollary 6.1.2. *Under the same assumptions, if $d = 1$, we have $\mathcal{O}_K \cdot \mathcal{O}_L = \mathcal{O}_{KL}$ and $\operatorname{disc}(KL) = \operatorname{disc}(K)^n \operatorname{disc}(L)^m$.*

To prove the proposition, we first establish the following lemma:

Lemma 6.1.3. *Assume $[KL : \mathbb{Q}] = mn$. Let σ be an embedding of K in $\mathbb{C}$ and let τ be an embedding of L in $\mathbb{C}$. Then there exists an embedding of KL in $\mathbb{C}$ which restricted to K is σ and restricted to L is τ.*

Proof. We know that σ has n distinct extensions to embeddings of KL in $\mathbb{C}$, say $\tilde{\sigma}_1, \ldots, \tilde{\sigma}_n$, and moreover $\tilde{\sigma}_i|_L \neq \tilde{\sigma}_j|_L$ for $i \neq j$ since otherwise $\tilde{\sigma}_i = \tilde{\sigma}_j$ on KL, but they're all distinct.

Hence $\tilde{\sigma}_i|_L$ give n distinct embeddings of L in $\mathbb{C}$, but there are only n distinct embeddings of L in $\mathbb{C}$ since $[L : \mathbb{Q}] = n$, so we must have $\tilde{\sigma}_i|_L = \tau$ for some i. □

Date: January 25th, 2018.

Proof of proposition. Let $\{\alpha_1, \alpha_2, \ldots, \alpha_m\}$ be an integral basis for $\mathcal{O}_K$ and let $\{\beta_1, \beta_2, \ldots, \beta_n\}$ be an integral basis for $\mathcal{O}_L$. Then $\{\alpha_i\beta_j\}$ for $1 \leq i \leq m$ and $1 \leq j \leq n$ is a basis for KL over $\mathbb{Q}$. It is also a basis for $\mathcal{O}_K \cdot \mathcal{O}_L$ over $\mathbb{Z}$, and $\{\alpha_i\beta_j\} \subset \mathcal{O}_{KL}$.

By Theorem 4.2.3, for $\gamma \in \mathcal{O}_{KL}$ we can write

$$\gamma = \sum_{i,j} \frac{a_{ij}}{M} \alpha_i \beta_j$$

where $M, a_{ij} \in \mathbb{Z}$ and we have reduced in such a way that

$$\gcd(M, a_{11}, \ldots, a_{mn}) = 1,$$

and we know that $M \mid \operatorname{disc}(\alpha_i\beta_j)$.

Our goal is to show that $M \mid d$ since then $\mathcal{O}_{KL} \subset \frac{1}{d}\mathcal{O}_K\mathcal{O}_L$.

Let $\sigma_1, \sigma_2, \ldots, \sigma_n$ be the embeddings of K in $\mathbb{C}$. For each σ_i there is an extension $\tilde{\sigma}_i$ to KL such that $\tilde{\sigma}_i|_L = \mathrm{Id}_L$ by the lemma. Apply this to γ above, whence

$$\tilde{\sigma}_k(\gamma) = \sum_{i,j} \frac{a_{ij}}{M} \sigma_k(\alpha_i)\beta_j = \sum_j \sigma_k(\alpha_i) x_i$$

where

$$x_i = \sum_j \frac{a_{ij}}{M} \beta_j.$$

Setting this up as a matrix equation we have

$$\big[\sigma_k(\alpha_i)\big] \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_m \end{bmatrix} = \begin{bmatrix} \tilde{\sigma}_1(\gamma) \\ \tilde{\sigma}_2(\gamma) \\ \vdots \\ \tilde{\sigma}_m(\gamma) \end{bmatrix}$$

which we solve using Cramer's rule by taking $\delta = \det([\sigma_k(\alpha_i)])$, so $\delta^2 = \operatorname{disc}(K)$ and letting γ_i be the determinant of $[\sigma_k(\alpha_i)]$ with the ith column replaced by the right-hand side above. Then $x_i = \gamma_i/\delta$. Note that $\delta, \gamma_i \in A$, the algebraic integrals in $\mathbb{C}$, and so

$$\operatorname{disc}(K) x_i = \delta^2 \frac{\gamma_i}{\delta} = \delta x_i \in A,$$

but the left-hand side is

$$\sum_j \frac{\operatorname{disc} K a_{ij}}{M} \beta_j \in L \cap A = \mathcal{O}_L$$

since β_j form an integral basis for $\mathcal{O}_L$. Hence

$$\frac{\operatorname{disc}(K) a_{ij}}{M} \in \mathbb{Z},$$

so $M \mid \operatorname{disc}(K)$ since by construction M and a_{ij} are all coprime. By the exact same argument but replacing K with L we have $M \mid \operatorname{disc}(L)$, so $M \mid \gcd(\operatorname{disc}(K), \operatorname{disc}(L))$.

If $d = 1$, then $M = \pm 1$, so $\{\alpha_i\beta_j\}$ is an integral basis for $\mathcal{O}_{KL}$, and then by computation

$$\operatorname{disc}(KL) = \operatorname{disc}(\alpha_i\beta_j) = \operatorname{disc}(K)^n \operatorname{disc}(L)^m. \qquad \square$$

Corollary 6.1.4. *Let $K = \mathbb{Q}(\xi_m)$ with $\xi_m = e^{2\pi i/m}$. Then $\mathcal{O}_K = \mathbb{Z}[\xi_m]$.*

Proof. It suffices to consider $m = p_1^{r_1} p_2^{r_2}$ with p_1 and p_2 distinct primes. Let $m_1 = p_1^{r_1}$ and $m_2 = p_2^{r_2}$, and let $K_1 = \mathbb{Q}(\xi_{m_1})$ and $K_2 = \mathbb{Q}(\xi_{m_2})$. Then $\mathcal{O}_{K_1} = \mathbb{Z}[\xi_{m_1}]$ and $\mathcal{O}_{K_2} = \mathbb{Z}[\xi_{m_2}]$. Note that $\gcd(m_1, m_2) = 1$ and $\xi_m^{m_1} = \xi_{m_2}$ and $\xi_m^{m_2} = \xi_{m_1}$, and so $\xi_m = \xi_{m_1}^s \xi_{m_2}^t$ where $sm_1 + tm_2 = 1$, $s, t \in \mathbb{Z}$.

Since $\operatorname{disc}(K_i) \mid m_i^{\varphi(m_i)}$, we have $\gcd(\operatorname{disc}(K_1), \operatorname{disc}(K_2)) = 1$, and hence by the corollary above $\mathcal{O}_K = \mathcal{O}_{K_1} \cdot \mathcal{O}_{K_2} = \mathbb{Z}[\xi_{m_1}]\mathbb{Z}[\xi_{m_2}] = \mathbb{Z}[\xi_m]$. □

Remark 6.1.5. With $K = \mathbb{Q}(\alpha) \subset \mathcal{O}_K$, we do not in general have $\mathcal{O}_K = \mathbb{Z}[\alpha]$.

6.2 Prime Decomposition in Rings of Integers

Before proceeding we need some prerequisites from commutative algebra.

Definition 6.2.1 (Dedekind domain)**.** A ***Dedekind domain*** D is a Noetherian, integrally closed domain of dimension 1.

Definition 6.2.2 (Noetherian ring)**.** A ***Noetherian ring*** R is a ring that satisfies the ascending chain condition, meaning that a chain of ideals

$$I_1 \subset I_2 \subset I_3 \subset \dots$$

is stationary, i.e. eventually $I_k = I_{k+1} = \dots$. This is in turn equivalent with every ideal $I \subset R$ being finitely generated as an R-module.

Definition 6.2.3 (Integrally closed)**.** Let D be an integral domain and let K be its quotient field. Then D is ***integrally closed*** if $\alpha \in K$ and $f(\alpha) = 0$ for some monic $f(x) \in D[x]$ implies $\alpha \in D$.

Definition 6.2.4 (Dimension 1)**.** A Noetherian domain R is of ***dimension 1*** if every nonzero prime ideal is maximal.

Theorem 6.2.5. *The ring $\mathcal{O}_K$ is a Dedekind domain.*

Proof. To see that $\mathcal{O}_K$ is Noetherian, take $I \subset \mathcal{O}_K \cong \mathbb{Z}^n$, with this isomorphism being as $\mathbb{Z}$-modules. Then I is finitely generated as a $\mathbb{Z}$-module, and since $\mathbb{Z} \subset \mathcal{O}_K$, it is also finitely generated as an $\mathcal{O}_K$-module.

By definition of $\mathcal{O}_K$, it is the integral closure of $\mathbb{Z}$ in K and hence it is integrally closed.

Finally to see that $\mathcal{O}_K$ is of dimension 1, take $P \subset \mathcal{O}_K$ a nonzero prime ideal. We want to show that P is maximal, which is equivalent to $\mathcal{O}_K/P$ being a field. Since P is prime by assumption, we know first of all that $\mathcal{O}_K/P$ is an integral domain.

It suffices to show that $\mathcal{O}_K/P$ is finite since every finite integral domain is a field. Let $\alpha \neq 0$ in P and let $\mathbb{Z} \ni m = \mathrm{N}_{K/\mathbb{Q}}(\alpha) = \alpha\beta$, where by β we mean the product of the remaining Galois conjugates of α. Then

$$\beta = \frac{m}{\alpha} \in K \cap A = \mathcal{O}_K$$

whence $m = \alpha\beta \in P$, since $\alpha \in P$ and $\beta \in \mathcal{O}_K$. Hence $(m) \subset P \subset \mathcal{O}_K$, and so

$$\left|\frac{\mathcal{O}_K}{P}\right| \leq \left|\frac{\mathcal{O}_K}{(m)}\right| = \left|\frac{\mathbb{Z}^n}{n\mathbb{Z}^n}\right| < \infty$$

by the aforementioned isomorphism. □

Definition 6.2.6. Let D be a Dedekind domain and K its field of fractions. Let $I, J \subset D$ be ideals.

We say that I ***divides*** J, denoted $I \mid J$ if $I \supset J$. We also call $\gcd(I, J) = I + J$, $\operatorname{lcm}(I, J) = I \cap J$, and

$$IJ = \left\{ \sum_i a_i b_i \;\middle|\; a_i \in I, b_i \in J \right\}$$

and then $I \cap J = IJ$ if $\gcd(I, J) = 1 = (1) = D$, i.e. I and J are coprime.

Lecture 7 Ideal Factorisation

7.1 Unique Factorisation of Ideals

In the following discussion, D is a Dedekind domain and K is its field of fractions.

Lemma 7.1.1. *For every ideal $I \subset D$, $I \neq 0$, there exists nonzero prime ideals $P_1, P_2, \ldots, P_r$ such that*

$$P_1 \cdot P_2 \cdot \ldots \cdot P_r \subset I,$$

$P_1, P_2, \ldots, P_r$ not necessarily distinct.

Note how this corresponds to how every integer has at least one prime factor.

Proof. Let S be the set of proper ideals of D for which the assumption in the lemma is false. Assume $S \neq \varnothing$—we clearly wish for this to lead to a contradiction.

Since D is Noetherian, S has a maximal element, say M. Then M is not a prime ideal, for otherwise it is its own factor P_1 above.

Hence there exists some $b_1, b_2 \in D \setminus M$ such that $b_1 b_2 \in M$. Now consider $I_1 = (b_1) + M \supsetneq M$ and $I_2 = (b_2) + M \supsetneq M$. Since M is maximal in S, we must have $I_1, I_2 \notin S$.

Therefore they do contain products of prime ideals, so there exist $P_1 \cdot P_2 \cdot \ldots \cdot P_r \subset I_1$ and $Q_1 \cdot Q_2 \cdot \ldots \cdot Q_s \subset I_2$, where P_i and Q_j are prime ideals.

Then

$$P_1 P_2 \cdots P_r Q_1 Q_2 \cdots Q_s \subset I_1 I_2 \subset M,$$

since $b_1 b_2 \in M$, which is a contradiciton. Hence $S = \varnothing$. □

Lemma 7.1.2. *Let P be a nonzero prime ideal in D and define*

$$P^{-1} = \{\, x \in K \mid xP \subset D \,\}.$$

Then $IP^{-1} \neq I$ for every nonzero ideal $I \subset D$.

Note that

$$IP^{-1} = \left\{ \sum_{i=1}^{r} a_i x_i \;\middle|\; a_i \in I, x_i \in P^{-1} \right\}$$

so, for example,

$$P^{-1} = (p\mathbb{Z})^{-1} = \frac{1}{p}\mathbb{Z}$$

in $\mathbb{Z}$.

Date: January 30th, 2018.

Proof. We claim first that $P^{-1} \not\subset D$. Let $0 \neq a \in P$ with $(a) \subsetneq P$. Take

$$P_1 P_2 \cdots P_r \subset (a) \subsetneq P$$

with r as small as possible, which is of course possible by the above lemma. Note $r \geq 2$.

Then if $P_i \not\subset P$ for every $i = 1, 2, \ldots, r$, then there exist $\alpha_i \in P_i$, hence $\alpha_i \in P$ for every $i = 1, 2, \ldots, r$, such that

$$\alpha_1 \alpha_2 \cdots \alpha_r \notin P.$$

But since P is a prime ideal, this is a contradiction. Hence $P_i \subset P$ for some i. But in a Dedekind domain every nonzero prime ideal is maximal, so $P_i = P$.

Without loss of generality, let us assume $P_1 = P$ (if not, just rearrange and relabel).

Now $P_2 P_3 \cdots P_r \not\subset (a)$ since r was chosen as small as possible.

Take $b \in P_2 P_3 \cdots P_r$, $b \notin (a)$. Then

$$\frac{b}{a} P \subset D,$$

which means by definition that $b/a \in P^{-1}$, but $b/a \notin D$ since $b \notin (a)$.

Now let $I \neq 0$, $I \subset D$, and let $\alpha_1, \alpha_2, \ldots, \alpha_n$ be the generators of I as a D-module (which must exist since D is Noetherian). Suppose $IP^{-1} = I$.

For any $x \in P^{-1}$, we have

$$x\alpha_i = \sum_{j=1}^{n} a_{ij} \alpha_j$$

with $a_{ij} \in D$. Let $A = [a_{ij}]$ and so

$$A \begin{bmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{bmatrix} = x \begin{bmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{bmatrix}$$

meaning that

$$(xI - A) \begin{bmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{bmatrix} = 0$$

and so $\det(xI - A) = 0$, and expanding this determinant we get some monic polynomial $x^n + \ldots \in D[x]$, whence x is integral over D.

Since D is Dedekind it is also integrally closed, meaning that $x \in D$, whereby $P^{-1} \subset D$. That's a contradiction, which means that $IP^{-1} \neq I$. □

Theorem 7.1.3. *Every nonzero proper ideal $I \subsetneq D$ had a unique factorisation*

$$I = P_1^{e_1} P_2^{e_2} \cdots P_r^{e_r}$$

with $e_i > 0$ and P_i distinct primes.

Proof. We start with the existence proof. Let S be the set of nonzero proper ideals in D such that they do not have a prime factorisation. Assume, as before, that $S \neq \varnothing$. Then since D is Noetherian there must be a maximal element in S, call it M. Then we must have $M \subset P \subset D$ for some maximal (and prime) ideal P.

By definition, $D \subset P^{-1}$, and by the lemma

$$M \subsetneq MP^{-1} \subset PP^{-1} = D.$$

The last equality comes from $P \subset PP^{-1} \subset D$, and since P is maximal we must have $P = PP^{-1}$ or $PP^{-1} = D$, and by the lemma it can't be the former.

Since $M \subsetneq P$, and $MP^{-1} \neq D$, for otherwise $MP^{-1} = D$ which implies $P = DP = MP^{-1}P = M$, which is a contradiction.

Thus $M \subsetneq MP^{-1} \subsetneq D$, and since M is maximal in S this means that $MP^{-1} \notin S$, so it by assumption has a unique prime factorisation, say

$$MP^{-1} = P_1^{e_1} P_2^{e_2} \cdots P_r^{e_r},$$

where P_i are prime ideals and $e_i > 0$. But if we just multiply by P we get

$$M = PP_1^{e_1} P_2^{e_2} \cdots P_r^{e_r}$$

which is a contradiction since $M \in S$, and so therefore $S = \varnothing$.

Now let us consider uniqueness. Suppose

$$I = P_1^{e_1} P_2^{e_2} \cdots P_r^{e_r} = Q_1^{a_1} Q_2^{a_2} \cdots Q_s^{a_2}.$$

This means that

$$Q_1^{a_1} Q_2^{a_2} \cdots Q_s^{a_2} \subset P_1$$

implying that $Q_i = P_i$ for some i; let's say $Q_1 = P_1$. Then

$$P_1^{-1} I = P_1^{e_1 - 1} P_2^{e_2} \cdots P_r^{e_r} = Q_1^{a_1 - 1} Q_2^{a_2} \cdots Q_s^{a_2}.$$

Repeat this, yielding eventually $P_i = Q_i$, $e_i = a_i$, and $r = s$. □

Note that the uniqueness proof is essentially the same as the standard proof of the same for integers.

Note also that, as with integers, it is often very hard to actually factor ideals, even though we know we can.

Definition 7.1.4 (Fractional ideal)**.** Let D be a Dedekind domain and K its field of fractions. A ***fractional ideal*** of K is a finitely generated D-submodule of K.

Example 7.1.5. Any ideal $I \subset D$ is a fractional ideal. In particular, these are called ***integral ideals*** of K. ▲

Remark 7.1.6. Consider $I = (\alpha_1, \alpha_2, \ldots, \alpha_k)$ as a D-module, with $\alpha_i \in K$. Then there exist $d_i \in D$ such that $d_i \alpha_i \in D$, and so there exists a common denominator $d \in D$ such that dI is an integral ideal.

Lemma 7.1.7. *For any ideal $I \subset D$, $I \neq 0$,*

$$I^{-1} = \{\, x \in K \mid xI \subset D \,\}$$

is a fractional ideal.

Proof. Let $x \neq 0$ in I. Then $xI^{-1} \subset D$ by the definition of I^{-1}. Since D is Noetherian, we moreover know that xI^{-1} is finitely generated as a D-module, say by $x\alpha_1, x\alpha_2, \ldots, x\alpha_n$. Then for any $y \in I^{-1}$ we have

$$xy = \sum_{i=1}^{n} a_i x \alpha_i$$

where $a_i \in D$. Since D is an integral domain, we have cancellation laws, so

$$y = \sum_{i=1}^{n} a_i \alpha_i,$$

meaning that I^{-1} is generated by $\alpha_1, \alpha_2, \ldots, \alpha_n$ as a D-module, whence it's a fractional ideal. □

Theorem 7.1.8. *Let I_K denote the set of all nonzero fractional ideals of K. Then I_K is an abelian group under multiplication with identity $D = (1)$ and the inverse of $I \subset I_K$ is $I^{-1} = \{ x \in K \mid xI \subset D \}$.*

Proof. First we prove that it is closed under multiplication. For any $I, J \in I_K$, if I is generated by $\alpha_1, \alpha_2, \ldots, \alpha_n$ and J by $\beta_1, \beta_2, \ldots, \beta_m$, then IJ is generated by $\alpha_i \beta_j$. Hence $IJ \in I_K$.

Secondly, let us show that $D = (1)$ is the identity, i.e. that $DI = I$ for any $I \subset I_K$. But this is immediately true since I is a D-module.

Finally let us verify that the inverse does what it should. Let P be a prime ideal in D. Then $P \subsetneq PP^{-1} \subset D$, with the previous lemma guarantueeing $P \subsetneq PP^{-1}$. Now since P is maximal, we must have $PP^{-1} = D$.

For $I \subset D$, use the prime factorisation to conclude $II^{-1} = D$.

Now for general $I \in I_K$, there exists some $d \in D$ such that $dI \subset D$, so $(dI)(dI)^{-1} = D$. □

Remark 7.1.9. Every nonzero fractional ideal I has a unique factorisation

$$I = P_1^{e_1} P_2^{e_2} \cdots P_k^{e_k}$$

where, as compared to $I \subset D$, $e_i \in \mathbb{Z} \setminus \{ 0 \}$, i.e. we allow negative powers.

In other words I_K is a free abelian group on the set of nonzero prime ideals of D.

Definition 7.1.10 (Principal fractional ideal)**.** The ***principal fractional ideals*** of K are the D-modules in K of the form $xD = (x)$, with $x \in K$. Let P_K denote the set of nonzero principal fractional ideals in K. Then P_K is a subgroup of I_K.

Definition 7.1.11 (Class group, class number)**.** The ***class group*** of K is $\mathrm{Cl}(K) = I_K / P_K$. Moreover $h(K) = \#\,\mathrm{Cl}(K)$ is called the ***class number*** of K.

Remark 7.1.12. The class group $\mathrm{Cl}(K)$ measures the failure of unique factorisation in D, since if $\mathrm{Cl}(K)$ is trivial, i.e. $h(K) = 1$, then D is a principal ideal domain, which for a Dedekind domain means its a unique factorisation domain.

We will show later that if K is a number field, then $h(K) < \infty$.

Example 7.1.13. Note that prime ideals in $\mathbb{Z}$ are not, when lifted, necessarily prime ideal in number fields. Suppose, say $K = \mathbb{Q}(\sqrt{-5})$, and consider

$$\begin{array}{ccccc} K & \supset & \mathcal{O}_K = \mathbb{Z}[\sqrt{-5}] & \supset & 2\mathcal{O}_K = (2, 1+\sqrt{-5})^2 \\ | & & & & \\ \mathbb{Q} & \supset & \mathbb{Z} & \supset & 2\mathbb{Z}. \end{array}$$

Here $2\mathbb{Z}$ is a prime ideal in $\mathbb{Z}$, but $2\mathcal{O}_K$ is not a prime ideal in $\mathcal{O}_K$. However, $(2, 1+\sqrt{-5})$ is. ▲

Lecture 8 Ramification

8.1 Ramification Index

Given a number field K, with a prime ideal $p\mathbb{Z}$ in $\mathbb{Z} \subset \mathbb{Q}$, it in general won't be the case that $p\mathcal{O}_K$ is a prime. However, by the discussion last time, it must be the case that

$$p\mathcal{O}_K = q_1^{e_1} q_2^{e_2} \cdots q_r^{e_r}$$

where $q_i \subset \mathcal{O}_K$ are prime ideals.

Definition 8.1.1 (Ramification)**.** Let $L \supset K$ be number fields. Let $P \subset \mathcal{O}_K$ be a prime ideal.

(*i*) If $P\mathcal{O}_L = q_1^{e_1} q_2^{e_2} \cdots q_r^{e_r}$, then e_i is called the ***ramification index*** of P at q_i. We denote this by $e(q_i/P)$.

(*ii*) The prime P is said to be ***ramified*** in L if some $e_i > 1$.

Proposition 8.1.2. *Let $L \supset K$ be number fields. Let $P \subset \mathcal{O}_K$ be a prime in $\mathcal{O}_K$, and $q \subset \mathcal{O}_L$ be a prime in $\mathcal{O}_L$. The following are equivalent:*

(*i*) *$q \mid P\mathcal{O}_L$, i.e. $P\mathcal{O}_L \subset q$;*

(*ii*) *$q \supset P$;*

(*iii*) *$q \cap \mathcal{O}_K = P$; and*

(*iv*) *$q \cap K = P$.*

Remark 8.1.3. We say that q ***lies over*** P or P ***lies under*** q in the above proposition.

Proof. (*i*) and (*ii*) are trivially equivalent by definition. Likewise (*iii*) and (*iv*) are equivalent since $q \subset \mathcal{O}_L$ and $\mathcal{O}_L \cap K = \mathcal{O}_K$.

(*iii*) implies (*ii*) again trivially, and finally (*ii*) implies (*iii*) by noting that $P \subset q \cap \mathcal{O}_K \subsetneq \mathcal{O}_K$, because it $q \cap \mathcal{O}_K = \mathcal{O}_K = (1)$, then $1 \in q$ meaning that $q = \mathcal{O}_L$, a contradiction. So P in the left-hand side is nonzero, making it maximal, so $P = q \cap \mathcal{O}_K$. □

Theorem 8.1.4. *Let $L \supset K$ be number fields.*

Date: February 1st, 2018.

(*i*) *Every prime $q \subset \mathcal{O}_L$ lies over a unique prime $P \subset \mathcal{O}_K$.*

(*ii*) *Every prime $P \subset \mathcal{O}_K$ lies under at least one prime $q \subset \mathcal{O}_L$.*

Proof. (*i*) follows from $q \cap \mathcal{O}_K$ being a prime in $\mathcal{O}_K$. Similarly, (*ii*) follows from $P\mathcal{O}_L \neq \mathcal{O}_L$, hence has a prime factorisation.

Suppose $P\mathcal{O}_L = \mathcal{O}_L$. Then $1 \in P\mathcal{O}_L$. Consider $P^{-1} \subset K$, $P^{-1} \not\subset \mathcal{O}_K$. Then there exists some $e \in K \setminus \mathcal{O}_K$, $r \in P^{-1}$, i.e. $rP \in \mathcal{O}_K$.

Then $rP\mathcal{O}_L \subset \mathcal{O}_K\mathcal{O}_L = \mathcal{O}_L$, but $1 \in P\mathcal{O}_L$, meaning that $r \in \mathcal{O}_L \cap K = \mathcal{O}_K$, a contradiction. □

In light of this, consider the following setting:

$$\begin{array}{ccccc} L & \supset & \mathcal{O}_L & \supset & q \\ | & & & & | \\ K & \supset & \mathcal{O}_K & \supset & P. \end{array}$$

Consider the ring homomorphism

$$\varphi \colon \mathcal{O}_K \to \frac{\mathcal{O}_L}{q},$$

where since q is a nonzero prime ideal it is also maximal, whence $\mathcal{O}_L/q$ is a field. The kernel of this map is $\ker \varphi = \mathcal{O}_K \cap q = P$, so this induces a homomorphism

$$\bar{\varphi} \colon \frac{\mathcal{O}_K}{P} \hookrightarrow \frac{\mathcal{O}_L}{q}$$

where both of the above quotients are fields.

Hence

$$\begin{array}{c} \frac{\mathcal{O}_L}{q} \\ | f \\ \frac{\mathcal{O}_K}{P} \end{array}$$

is a field extension. We call $\mathcal{O}_L/q$ the ***residue field*** associated with q.

The dimension of $\mathcal{O}_L/q$ over $\mathcal{O}_K/P$ as a fector space is called the ***inertial degree*** of q over P, denoted $f(q/P)$.

Example 8.1.5. Consider

$$\begin{array}{ccccccc} K = \mathbb{Q}(i) & \supset & \mathbb{Z}[i] = \mathcal{O}_K \supset 2\mathcal{O}_K = (1-i)^2 & & & & \\ | & & & & & & \\ \mathbb{Q} & \supset & \mathbb{Z} & & \supset & & (2), \end{array}$$

where we then consider

$$\begin{array}{c} \frac{\mathbb{Z}[i]}{(1-i)} \\ | \\ \frac{\mathbb{Z}}{2\mathbb{Z}}. \end{array}$$

Then we have $2\mathcal{O}_K = (1-i)^2$, so $e((1-i)/2) = 2$ and

$$\Big|\frac{\mathbb{Z}[i]}{(1-i)}\Big| = 2$$

and $|\mathbb{Z}/2\mathbb{Z}| = 2$, so $f((1-i)/2) = 1$. ▲

Exercise 8.1.6. As expected, if we let $M \supset L \supset K$ be number fields, and let $R \supset q \supset P$ be primes in $\mathcal{O}_M \supset \mathcal{O}_L \supset \mathcal{O}_K$ respectively, such that

$$\begin{array}{ccccc} M & \supset & \mathcal{O}_M & \supset & R \\ | & & & & | \\ L & \supset & \mathcal{O}_L & \supset & q \\ | & & & & | \\ K & \supset & \mathcal{O}_K & \supset & P, \end{array}$$

we have

$$e(R/P) = e(R/q)e(q/P)$$

and

$$f(R/P) = f(R/q)f(q/P).$$

Theorem 8.1.7. *Let*

$$\begin{array}{ccccc} L & \supset & \mathcal{O}_L & \supset & P\mathcal{O}_L = q_1^{e_1} q_2^{e_2} \cdots q_r^{e_r} \\ \Big|{\scriptstyle n} & & & & \\ K & \supset & \mathcal{O}_K & \supset & P \end{array}$$

and hence

$$\begin{array}{c} \mathcal{O}_L/q_i \\ \Big|{\scriptstyle f_i} \\ \mathcal{O}_K/P \end{array}$$

with $f_i = f(q_i/P)$ and $e_i = e(q_i/P)$. Then

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

Before we prove this, let us define a new notion and state a proposition which we'll prove alongside the theorem.

Definition 8.1.8 (Norm of ideal)**.** Let K be a number field and let $I \subset \mathcal{O}_K$ be an ideal. The ***norm*** of I is

$$\mathrm{N}(I) = \mathrm{N}_K(I) = \Big|\frac{\mathcal{O}_K}{I}\Big|.$$

Proposition 8.1.9. *Let $L \supset K$ be number fields with $[L:K] = n$.*

(*i*) *For ideals $I, J \subset \mathcal{O}_K$, $\mathrm{N}(IJ) = \mathrm{N}(I)\,\mathrm{N}(J)$.*

(*ii*) *Let $I \subset \mathcal{O}_K$. Then $\mathrm{N}_L(I\mathcal{O}_L) = \mathrm{N}_K(I)^n$.*

(*iii*) *Let $\alpha \neq 0$, $\alpha \in \mathcal{O}_K$. For the principal ideal (α) we have $N_K((\alpha)) = |N_{K/\mathbb{Q}}(\alpha)|$, where the first norm is that of an ideal, and the second is that of an element.*

Proof. We start by proving (i) from the proposition. First assume I and J are coprime, i.e. $I+J = \mathcal{O}_K$, or equivalently $IJ = I \cap J$. By the Chinese remainder theorem we have that $\mathcal{O}_K/IJ = \mathcal{O}_K/I \cap J$ is isomorphic to $\mathcal{O}_K/I \times \mathcal{O}_K/J$. Hence

$$\Big|\frac{\mathcal{O}_K}{IJ}\Big| = \Big|\frac{\mathcal{O}_K}{I}\Big| \cdot \Big|\frac{\mathcal{O}_K}{J}\Big|,$$

whereby $\mathrm{N}(IJ) = \mathrm{N}(I)\,\mathrm{N}(J)$.

Secondly, assume $I = P^m$ for $P \subset \mathcal{O}_K$ prime, i.e. I is a prime power. Then the goal is to show that $\mathrm{N}(I) = \mathrm{N}(P)^m$, and

$$\mathrm{N}(I) = \Big|\frac{\mathcal{O}_K}{P^m}\Big|$$

by definition. Now note that

$$\mathcal{O}_K \supset P \supset P^2 \supset P^3 \supset \ldots \supset P^m,$$

where the norm between each is $N(P)$. Hence the claim is true if

$$\mathrm{N}(P) = \Big|\frac{\mathcal{O}_K}{P}\Big| = \Big|\frac{P^k}{P^{k+1}}\Big|.$$

Fix any $\alpha \in P^k \setminus P^{k+1}$, i.e. nonzero in the latter quotient. We have an isomorphism

$$\mathcal{O}_K/P \to \alpha\mathcal{O}_K/\alpha P$$

which is induced by the natural projection $\mathcal{O}_K \to \alpha\mathcal{O}_K/\alpha P$. Now consider the homomorphism $\varphi\colon \alpha\mathcal{O}_K \to P^k/P^{k+1}$, which is the natural inclusion since $\alpha\mathcal{O}_K \subset P^k$.

Then $\ker\varphi = \alpha\mathcal{O}_K \cap P^{k+1} = \alpha P$, and

$$\operatorname{Im}\varphi = \frac{\alpha\mathcal{O}_K + P^{k+1}}{P^{k+1}} = \frac{P^k}{P^{k+1}}$$

since $P^{k+1} \subsetneq \alpha\mathcal{O}_K + P^{k+1} = P^k$.

Therefore φ induces an isomorphism between $\alpha\mathcal{O}_K/(\alpha P)$ and P^k/P^{k+1}, whence

$$\Big|\frac{\mathcal{O}_K}{P}\Big| = \Big|\frac{\alpha\mathcal{O}_K}{\alpha P}\Big| = \Big|\frac{P^k}{P^{k+1}}\Big|.$$

Hence N is multiplicative for coprime ideals and prime powers, so for two arbitrary ideals, first factor them, then apply these two.

Next let us tackle the theorem for the special case $K = \mathbb{Q}$. Then $P = p\mathbb{Z}$, with p a prime, and

$$\mathrm{N}_L(p\mathcal{O}_L) = \mathrm{N}(q_1)^{e_1}\,\mathrm{N}(q_2)^{e_2}\cdots\mathrm{N}(q_r)^{e_r}$$

by the above. Hence $\mathrm{N}(q_i) = p^{f_i}$, and

$$\mathrm{N}_L(p\mathcal{O}_L) = \prod_{i=1}^{r} p^{f_i e_i} = p^{\sum_{i=1}^{r} f_i e_i}.$$

Moreover

$$\mathrm{N}_L(p\mathcal{O}_L) = \Big|\frac{\mathcal{O}_L}{p\mathcal{O}_L}\Big| = \Big|\frac{\mathbb{Z}^n}{p\mathbb{Z}^n}\Big| = p^n,$$

whereby

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

so the theorem holds for $K = \mathbb{Q}$. □

Lecture 9 Ramification Index continued

9.1 Proof, continued

We showed last time that the theorem we are working on is true for $K = \mathbb{Q}$.

Now let us use what we know so far to tackle the second part of the proposition, but first a lemma:

Lemma 9.1.1. *Let D be a Dedekind domain with the field of fractions K. Let $B \subset A \subsetneq D$ be ideals. Then there exists $r \in K$ such that $rB \subset D$ but $rB \not\subset A$.*

Proof. We know from last time that $BB^{-1} = (1) = D$, where B^{-1} is a fractional ideal. Hence there exists some $\alpha \in D$ such that $\alpha B^{-1} \subset D$, and hence $(\alpha B^{-1})B = \alpha D$. Now since $A \subsetneq D$ we have $aA \subsetneq \alpha D$, and we select $\beta \in \alpha B^{-1}$ such that $\beta B \subset \alpha D$ but $\beta B \not\subset \alpha A$.

Take $r = \beta/\alpha$. Then $rB = \beta/\alpha B \subset D$ but $rB \not\subset A$. □

Proof of Proposition (ii). Since N is multiplicative, it suffices to consider $I = P$, a prime ideal. Then

$$\begin{array}{c} \mathcal{O}_L/P\mathcal{O}_L \\ \Big| m \\ \mathcal{O}_K/P \end{array}$$

where $\mathcal{O}_L/P\mathcal{O}_L$ is a vector space over $\mathcal{O}_K/P$ since the latter is a field. Our goal is to prove that the dimension of this vector space is n.

First let us establish that the dimension is bounded above by n, i.e.

$$[\mathcal{O}_L/P\mathcal{O}_L : \mathcal{O}_K/P] \leq n.$$

Let $\alpha_1, \alpha_2, \ldots, \alpha_{n+1} \in \mathcal{O}_L$. We then want to show that the corresponding elements in $\mathcal{O}_L/P\mathcal{O}_L$ are linearly dependent over $\mathcal{O}_K/P$.

Note first of all that the elements are linearly dependent over K, since $[L : K] = n$, and hence they are also linearly dependent over $\mathcal{O}_K$ (to see this, find a common denominator of the linear sum in K). Hence

$$\beta_1\alpha_1 + \beta_2\alpha_2 + \ldots + \beta_{n+1}\alpha_{n+1} = 0$$

Date: February 6th, 2018.

for some $\beta_i \in \mathcal{O}_K$. It is then our goal to show that not all $\beta_i \equiv 0 \pmod{P}$.

Applying the lemma with $A = P$ and $B = (\beta_1, \beta_2, \ldots, \beta_{n+1})$, there exists some $r \in K$ such that $rB \subset \mathcal{O}_K$, i.e. $r\beta_i \in \mathcal{O}_K$ for all i, but at the same time $rB \not\subset P$, i.e. not all $r\beta_i \equiv 0 \pmod{P}$¿ Hence

$$(r\beta_1)\alpha_1 + (r\beta_2)\alpha_2 + \ldots + (r\beta_{n+1})\alpha_{n+1} = 0$$

and we are done.

Using this we can prove that in fact $[\mathcal{O}_L/P\mathcal{O}_L : \mathcal{O}_K/P] = n$. Consider $P \cap \mathbb{Z} = p\mathbb{Z}$, with p a prime number. Then

$$p\mathcal{O}_K = P_1^{e_1} P_2^{e_2} \cdots P_r^{e_r},$$

and one of them must be equal to P, say $P_1 = P$. Let $f_i = f(P_i/p)$, whence

$$p\mathcal{O}_L = p\mathcal{O}_K \cdot \mathcal{O}_L = \prod_{i=1}^{r} P_i^{e_i}\mathcal{O}_L$$

whence by the first part of the proposition

$$\mathrm{N}_L(p\mathcal{O}_L) = \prod_{i=1}^{r} \mathrm{N}_L(P_i\mathcal{O}_L)^{e_i}.$$

Set $n_i = [\mathcal{O}_L/P_i\mathcal{O}_L L\mathcal{O}_K/P_i]$. Then $n_i \leq n$ for all i by the first claim above, and $\mathrm{N}_L(P_i\mathcal{O}_L) = \mathrm{N}_K(P_i)^{n_i}$, and moreover $\mathrm{N}_K(P_i) = p^{f_i}$. Hence

$$\mathrm{N}_L(p\mathcal{O}_L) = \prod_{i=1}^{r} \mathrm{N}_K(P_i)^{n_i e_i} = \prod_{i=1}^{r} p^{f_i n_i e_i}.$$

But we also have

$$\mathrm{N}_L(p\mathcal{O}_L) = \Big|\frac{\mathcal{O}_L}{p\mathcal{O}_L}\Big| = \Big|\frac{\mathbb{Z}^{mn}}{p\mathbb{Z}^{mn}}\Big| = p^{mn},$$

where $m = [K : \mathbb{Q}]$, whereby

$$\sum_{i=1}^{r} f_i n_i e_i = nm,$$

and since the theorem is true for the base field being $\mathbb{Q}$ we have

$$\sum_{i=1}^{r} e_i f_i = m,$$

so, since $n_i \leq n$, we get $n_i = n$ for all i. □

We are finally ready to prove the general case of the theorem.

Proof of Theorem. Consider the factorisation $P\mathcal{O}_L = q_1^{e_1} q_2^{e_2} \cdots q_r^{e_r}$ in L. By (ii) in the proposition, $\mathrm{N}_L(P\mathcal{O}_L) = \mathrm{N}_K(¶)^n$, where $n = [L : K]$. At the same time

$$\mathrm{N}_L(P\mathcal{O}_L) = \prod_{i=1}^{r} \mathrm{N}_L(q_i)^{e_i} = \prod_{i=1}^{r} \mathrm{N}_K(P)^{f_i e_i} = \mathrm{N}_K(P)^{\sum_{i=1}^{r} f_i e_i},$$

so

$$\sum_{i=1}^{r} e_i f_i = n.$$ □

We end the lecture by proving the last part of the proposition.

Proof of Proposition (iii). Let M be a normal extension of $\mathbb{Q}$ containing K, say

$$\begin{array}{c} M \\ \Big| n \\ K \\ \Big| m \\ \mathbb{Q} \end{array}$$

and let $\sigma\colon K \hookrightarrow \mathbb{C}$ extend to $\bar{\sigma}\colon M \hookrightarrow \mathbb{C}$ (actually $\bar{\sigma}\colon M \hookrightarrow M$ since M is normal). Moreover $\bar{\sigma}(\mathcal{O}_M) = \mathcal{O}_M$, hence

$$\mathrm{N}_M(\alpha\mathcal{O}_M) = \mathrm{N}(\sigma(\alpha)\mathcal{O}_M)$$

for $\alpha \in K$. Let $a = \mathrm{N}_{K/\mathbb{Q}}(\alpha) = \sigma_1(\alpha)\sigma_2(\alpha)\cdots\sigma_m(\alpha) \in \mathbb{Z}$. Then

$$\mathrm{N}_M(a\mathcal{O}_M) = \mathrm{N}_M(\sigma_1(\alpha)\mathcal{O}_M)\,\mathrm{N}_M(\sigma_2(\alpha)\mathcal{O}_M)\cdots\mathrm{N}_M(\sigma_m(\alpha)\mathcal{O}_M)$$

and since the extension is Galois all the embeddings just permute themselves, so this is equal to

$$\mathrm{N}_M(\alpha\mathcal{O}_M)^m = \mathrm{N}_K(\alpha\mathcal{O}_K)^{mn}.$$

Now since $a \in \mathbb{Z}$ we have $\mathrm{N}_M(a\mathcal{O}_M) = \mathrm{N}_{\mathbb{Q}}(a\mathbb{Z})^{mn} = |a|^{mn}$, whence $\mathrm{N}_K(\alpha\mathcal{O}_K) = |a| = |\mathrm{N}_{K/\mathbb{Q}}(\alpha)|$. □

Lecture 10 Ramified Primes

10.1 When Do Primes Split

Proposition 10.1.1. *Let $L \supset K$ be a Galois extension, and let $G = \mathrm{Gal}(L/K)$. Then G acts transitively on the set of prime ideals q of $\mathcal{O}_L$ lying over $P \subset \mathcal{O}_K$.*

The idea, then, is that $P\mathcal{O}_L = q_1^{e_1}q_2^{e_2}\cdots q_r^{e_r}$ and if $\sigma \in \mathrm{Gal}(L/K)$, then $\sigma\colon L \to L$ and $\sigma(\mathcal{O}_L) = \mathcal{O}_L$. The proposition says that for each pair q_i and q_j there exists some $\sigma \in \mathrm{Gal}(L/K)$ such that $\sigma(q_i) = q_j$.

Proof. Suppose there exists q and q' being prime ideals in $\mathcal{O}_L$ lying above P such that $q \neq \sigma(q')$ for all $\sigma \in G$. Then by the Chinese remainder theorem there exists some $x \in \mathcal{O}_L$ such that

$$\begin{cases} x \equiv 0 & (\mathrm{mod}\ q) \\ x \equiv 1 & (\mathrm{mod}\ \sigma(q')) \end{cases}$$

for all $\sigma \in G$. Now

$$\mathrm{N}_{L/K}(x) = \prod_{\sigma\in G}\sigma(x) \in q \cap K = P,$$

meaning that $x \notin \sigma(q')$ for all $\sigma \in G$, so $\sigma^{-1}(x) \notin q'$ for every $\sigma \in G$.

Date: February 8th, 2018.

Therefore $\sigma(x) \notin q'$ for every $\sigma \in G$, so

$$\mathrm{N}_{L/K}(x) = \prod_{\sigma \in G} \sigma(x) \notin q'$$

since q' is prime, but $q' \cap K = P$, so this is a contradiction. □

Corollary 10.1.2. *Suppose $L \supset K$ is a Galois extension, and let $P \subset \mathcal{O}_K$ be a nonzero prime ideal. Let $q_1, q_2 \subset \mathcal{O}_L$ be two prime ideals lying over P. Then $e(q_1/P) = e(q_2/P)$ and $f(q_1/P) = f(q_2/P)$, and hence $[L : K] = ref$ where r is the number of primes $q \subset \mathcal{O}_L$ lying above P.*

The fundamental question we wish to ask and answer is this: Let K be a number field. For which primes $p \in \mathbb{Z}$ is p ramified in K, i.e. $e(q/p) > 1$ for some $q \in \mathcal{O}_K$?

The answer is very simple to state, but not nearly as simple to prove: p is ramified in K if and only if $p \mid \mathrm{disc}(K)$.

We will prove the forward direction today, and the converse much, much later.

Theorem 10.1.3. *Let p be a prime in $\mathbb{Z}$. Suppose p is ramified in a number field K. Then $p \mid \mathrm{disc}(K)$.*

Proof. Let $q \in \mathcal{O}_K$ lie above p with $e(q/p) > 1$. We have

$$p\mathcal{O}_K = q^e q_1^{e_1} q_2^{e_2} \cdots q_r^{e_r} = q(\underbrace{q^{e-1} q_1^{e_1} q_2^{e_2} \cdots q_r^{e_r}}_{=I}).$$

Then $p\mathcal{O}_K = qI$ with $p\mathcal{O}_K \subsetneq I$ and I is divisible by *all* primes in $\mathcal{O}_K$ lying above p by construction. Let L be a Galois extension of $\mathbb{Q}$ such that $K \subset L$, and let $\sigma_1, \sigma_2, \ldots, \sigma_n$ be the embeddings of K in $\mathbb{C}$. Each of them extends to L, call it $\bar{\sigma}_i$.

Let $\alpha_1, \alpha_2, \ldots, \alpha_n$ be any integral basis for $\mathcal{O}_K$, and let $d = \mathrm{disc}(K) = \mathrm{disc}(\alpha_1, \alpha_2, \ldots, \alpha_n)$.

Since $p\mathcal{O}_K \subsetneq I$, we can find $\alpha \in I \setminus p\mathcal{O}_K$. Write

$$\alpha = m_1\alpha_1 + m_2\alpha_2 + \ldots + m_n\alpha_n$$

with $m_i \in \mathbb{Z}$, not all $m_i \equiv 0 \pmod{p}$ since $\alpha \notin p\mathcal{O}_K$. Without loss of generality, say $m_1 \not\equiv 0 \pmod{p}$, i.e. $p \nmid m_1$.

Then

$$\mathrm{disc}(\alpha, \alpha_2, \alpha_3, \ldots, \alpha_n) = \mathrm{disc}(m_1\alpha_1, \alpha_2, \ldots, \alpha_n) = m_1^2 \,\mathrm{disc}(\alpha_1, \alpha_2, \ldots, \alpha_n).$$

It then suffices to show $p \mid \mathrm{disc}(\alpha, \alpha_2, \ldots, \alpha_n)$ since $p \nmid m_1$. Now fix any prime $P \subset \mathcal{O}_L$ lying above p. Then $\alpha \in I$ means that $\alpha \in q_i \subset \mathcal{O}_K$ lying above p for every i, and so $\alpha \in P_i \subset \mathcal{O}_L$ lie above p for every i too.

Hence

$$\alpha \in P_1 \cap P_2 \cap \ldots \cap P_s$$

whereby

$$\sigma(\alpha) \in P_1 \cap P_2 \cap \ldots \cap P_s$$

for every $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$. Fix $P = P_1$. Then $\sigma(\alpha) \in P$ for all $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$, and in particular $\sigma_i(\alpha) \in P$ for $\sigma_i \colon K \hookrightarrow \mathbb{C}$.

Hence

$$m_1^2 \operatorname{disc}(\alpha_1, \alpha_2, \ldots, \alpha_n) = \operatorname{disc}(\alpha, \alpha_2, \ldots, \alpha_n) \in P \cap \mathbb{Z} = p\mathbb{Z}$$

where the left-hand side is in $\mathbb{Z}$, so $p \mid \operatorname{disc}(\alpha, \alpha_2, \ldots, \alpha_n)$. □

Corollary 10.1.4. *Let $K = \mathbb{Q}(\alpha)$ with $\alpha \in \mathcal{O}_K$. Let $f(x)$ be the monic minimal polynomial of α over $\mathbb{Q}$. Suppose $p \in \mathbb{Z}$ is a prime such that $p \nmid \mathrm{N}_{K/\mathbb{Q}}(f'(\alpha))$. Then p is unramified in K.*

Proof. We have $K = \mathbb{Q}(\alpha) \supset \mathcal{O}_K \supset \mathbb{Z}[\alpha]$, and so

$$\operatorname{disc}(\alpha) = [\mathcal{O}_K : \mathbb{Z}[\alpha]]^2 \operatorname{disc}(K),$$

where the left-hand side is $\pm \mathrm{N}_{K/\mathbb{Q}}(f'(\alpha))$. Hence $p \nmid \mathrm{N}_{K/\mathbb{Q}}(f'(\alpha))$ implies $p \nmid \operatorname{disc}(K)$, and so by the contrapositive of the theorem p is unramified. □

Corollary 10.1.5. *There are only finitely many primes in $\mathbb{Z}$ that are ramified in a number field K.*

Corollary 10.1.6. *Let $L \supset K$ be number fields. Then there are only finitely many prime ideals that are unramified in $\mathcal{O}_L$.*

Example 10.1.7. Let $K = \mathbb{Q}(\sqrt{D})$, with D being square-free. We know that

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}[\sqrt{D}], & \text{if } D \not\equiv 1 \pmod 4, \\ \mathbb{Z}[\frac{1+\sqrt{D}}{2}] & \text{if } D \equiv 1 \pmod 4, \end{cases}$$

along with

$$\operatorname{disc}(K) = \begin{cases} 4D, & \text{if } D \not\equiv 1 \pmod 4, \\ D & \text{if } D \equiv 1 \pmod 4. \end{cases}$$

Let $p \in \mathbb{Z}$ be prime. Then

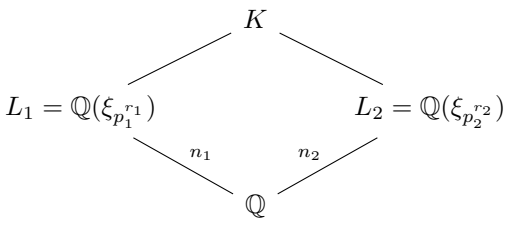
$$p\mathcal{O}_K = \begin{cases} P^2 & \text{if } p \mid \operatorname{disc}(K), \\ P & \text{if } p \nmid \operatorname{disc}(K), \left(\frac{\operatorname{disc}(K)}{p}\right) = -1, \\ P_1 P_2 & \text{if } p \nmid \operatorname{disc}(K), \left(\frac{\operatorname{disc}(K)}{p}\right) = 1. \end{cases}$$

We call the second case ***inert*** and the third case ***split***. ▲

Example 10.1.8. Consider the cyclotomic field $K = \mathbb{Q}(\xi_m)$ where $\xi_m = e^{2\pi i/m}$, and $m \geq 3$. We know that $\mathcal{O}_K = \mathbb{Z}[\xi_m]$.

First suppose $m = p^r$, with $p \in \mathbb{Z}$ a prime. Then we know that $\operatorname{disc}(K) \mid m^{\varphi(m)} = p^n$ for some power n, and so $\operatorname{disc}(K) = p^v$ for some power v. Hence p is the only prime ramified in K.

Next suppose $m = p_1^{r_1} p_2^{r_2}$, with $p_1 \neq p_2$ primes in $\mathbb{Z}$. Then as we know



and $\operatorname{disc}(K) = \operatorname{disc}(L_1)^{n_2} \operatorname{disc}(L_2)^{n_1} = p_2^{n_1} p_1^{n_2}$ so p is ramified in K if and only if $p \mid m$ where $m = p_1^{r_1} p_2^{r_2}$ for some powers r_1 and r_2.

Inductively, for any $m \geq 3$, p is ramified in $\mathbb{Q}(\xi_m)$ if and only if $p \mid m$. ▲

Note that if $K = \mathbb{Q}(\xi_m)$ we also have that K is a Galois extension of $\mathbb{Q}$, and so $p\mathcal{O}_K = (q_1 q_2 \cdots q_r)^e$ and $f = f(q_i/p)$ for all i, and so $ref = \varphi(m)$.

Now let us see if we can determine r, e, and f.

The first case to consider is $p \nmid m$. Then p is unramified in K, so $e = 1$, and we claim that f is the multiplicative order of p modulo m.

The way to think about this is that if $\gcd(p, m) = 1$, then $p \in (\mathbb{Z}/m\mathbb{Z})^\times$, whereby $p^f \equiv \pmod m$, so $r = \varphi(m)/f$.

So assume first that $m = q^k$ for $q \in \mathbb{Z}$ a prime such that $q \neq p$. Then if Q lies above P in $\mathcal{O}_K$, then

$$\begin{array}{c} \mathcal{O}_K/\mathbb{Q} = \mathbb{F}_{p^f} \\ \Big| f \\ \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p \end{array}$$

and $\operatorname{Gal}(\mathbb{F}_{p^f}/\mathbb{F}_p) = (\tau)$ is cyclic, and in particular $\tau(x) = x^p$ is the Frobenius automorphism, and naturally $|(\tau)| = f$.

On the other hand, $\operatorname{Gal}(K/\mathbb{Q}) \cong (\mathbb{Z}/m\mathbb{Z})^\times$ by the isomorphism $\sigma_1(x) = x^a$ corresponding to $a \pmod m$, and in particular $\sigma_p(x) = x^p$ corresponding to $p \pmod m$.

Lecture 11 The Ideal Class Group

11.1 When are Primes Ramified in Cyclotomic Fields

Let $K = \mathbb{Q}(\xi_m)$ and let $p \in \mathbb{Z}$ be a prime. Then p is ramified in K if and only if $p \mid m$.

We know that K is a Galois extension of $\mathbb{Q}$, so $p\mathcal{O}_K = (q_1 q_2 \cdots q_r)^e$, and $f = f(q_1/p) = \ldots = f(q_r/p)$. We therefore want to determine r, e, and f, knowing that $ref = n = \varphi(m)$.

Let us first consider the case $p \nmid m$, so that p is unramified, meaning that $e = 1$, and so $p\mathcal{O}_K = q_1 q_2 \cdots q_r$. We claim that f is the multiplicative order of p modulo m.

This makes sense since $p \nmid m$ means that $(p, m) = 1$, and thereby $p \in \mathbb{Z}_m^\times$, and we claim that f is the smallest positive integer such that $p^d \equiv 1 \pmod m$.

Assume $m = q^k$ for $q \in \mathbb{Z}$ a prime, but $p \neq q$. Let $\xi = \xi_{q^k}$.

We then have

$$\begin{array}{c} \mathcal{O}_K/q_1 \cong \mathbb{F}_{p^f} \\ \Big| f \\ \mathbb{Z}/p\mathbb{Z} \cong \mathbb{F}_p \end{array}$$

and $\operatorname{Gal}(\mathbb{F}_{p^d}/\mathbb{F}_p) = (\tau)$, where $\tau \colon \mathbb{F}_{p^f} \to \mathbb{F}_{p^f}$, $\tau(x) = x^p$ is the Frobenius automorphism, and of course $|(\tau)| = f$. We also have $\operatorname{Gal}(K/\mathbb{Z}) \cong (\mathbb{Z}/m\mathbb{Z})^\times$, by $\sigma_a(\xi) = \xi^a \leftrightarrow a \pmod m$, and so in particular $\sigma_p(\xi) = \xi^p \leftrightarrow p \pmod m$.

Date: February 11th, 2018.

The order of p modulo m is equal to the order of σ_p in $\mathrm{Gal}(K/\mathbb{Q})$. Hence we want to show that the order of σ_p in $\mathrm{Gal}(K/\mathbb{Q})$ is in turn equal to the order of τ in $\mathrm{Gal}(\mathbb{F}_{p^f}/\mathbb{F}_p)$.

This is the same as saying $\sigma_p^a = \mathrm{Id}$ if and only if $\tau^a = \mathrm{Id}$, for every $a \in \mathbb{N}$.

First $\sigma_p^a = \mathrm{Id}$ is equivalent with $\sigma_p^a(\xi) = \xi$ if and only if $\xi^{p^a} = \xi$ which is the case if and only if $p^a \equiv 1 \pmod{m}$ since ξ is a primitive mth root of unity.

Secondly, $\tau^a = \mathrm{Id}$ if and only if $\tau^a(\xi) \equiv \xi \pmod{q_1}$, if and only if $\xi^{p^a} \equiv \xi \pmod{q_1}$. We claim that this, in turn, is equivalent with $p^a \equiv 1 \pmod{m}$.

The reverse direction is trivial since ξ is an mth root of unity.

The forward direction is a little trickier. Assume $\xi^{p^a} \equiv \xi \pmod{q_1}$, and write $p^a \equiv b \pmod{m}$ for $0 \leq b < m$, meaning that $\xi^{p^a} = \xi^b$. Then $b \neq 0$ since otherwise $\xi = 1$ (and indeed $p \mid m$ if it's the case).

We have $\xi \in \mathcal{O}_K^\times = \mathbb{Z}[\xi]^\times$ since $\mathrm{N}(\xi) = 1$ (and $\xi^m = 1$). So $\xi^{p^a - 1} \equiv 1 \pmod{q_1}$, implying that $\xi^{b-1} \equiv 1 \pmod{q_1}$. Then

$$(1-\xi)(1-\xi^2)\cdots(1-\xi^{m-1}) = m$$

since

$$x^{m-1} + x^{m-2} + \ldots + x + 1 = (x-\xi)(x-\xi^2)\cdots(x-\xi^{m-1})$$

so we plug in $x = 1$.

Now if $b > 1$, $1 - \xi^{b-1}$ appears somewhere in the above, whence $m \in q_1 \cap \mathbb{Z} = p\mathbb{Z}$, but this is a contradiction since $p \nmid m$. Therefore $b = 1$.

So the order of σ_p is the same as the order of τ.

This same argument works for any $(m, p) = 1$¡ so for $p \nmid m$, with $e = 1$, we know f, and therefore we can find r.

Now consider instead the case $p \mid m$, whereby p is ramified in K, so

$$p\mathcal{O}_K = (q_1 q_2 \cdots q_r)^e$$

with $e > 1$. Assume $m = p^k$. We claim $p\mathcal{O}_K = (1-\xi)^{\varphi(m)}$.

We have $\mathrm{N}(1-\xi) = p$, and moreover

$$\mathrm{N}(1-\xi) = \prod_{\substack{(k,m)=1 \\ 1 \leq k < m}} (1-\xi^k) = \prod_{\substack{(k,m)=1 \\ 1 \leq k < m}} \tfrac{1-\xi^k}{1-\xi} \in \mathcal{O}_K^\times (1-\xi) = u(1-\xi)^{\varphi(m)},$$

so $p\mathcal{O}_K = u(1-\xi)^{\varphi(m)}\mathcal{O}_K = (1-\xi)^{\varphi(m)}$, so $ref = \varphi(m)$ and $e \geq \varphi(m)$ (because $(1-\xi)$ could in principle split), but since the we have $ref = \varphi(m)$ we must have $e = \varphi(m)$ and so $r = f = 1$, meaning that $(1-\xi)$ is a prime ideal in $\mathcal{O}_K$.

The case we haven't dealt with is the possibility that $m = p^k \cdot n$, where $(n, p) = 1$.

11.2 The Ideal Class Group and Unit Group

Let K be a number field and let I_K denote the set of fractional ideals in K and P_K denote the set of principal fractional ideals in K. The class group is $\mathrm{Cl}(K) = I_K/P_K$, and the class number is $h(K) = \#\,\mathrm{Cl}(K)$.

The goal of this discussion is to show that $h(K) < \infty$.

Theorem 11.2.1. *Let K be a number field. Then there exists $\lambda > 0$ (depending only on K) such that for every nonzero $I \subset \mathcal{O}_K$ there exists a nonzero $\alpha \in I$ with*

$$|\mathrm{N}_{K/\mathbb{Q}}(\alpha)| \leq \lambda\, \mathrm{N}_K(I).$$

Proof. Let $n = [K : \mathbb{Q}]$. Let $\alpha_1, \alpha_2, \ldots, \alpha_n$ be an integral basis for $\mathcal{O}_K$ and let $\sigma_1, \sigma_2, \ldots, \sigma_n$ be the embeddings of K in $\mathbb{C}$.

Set

$$\lambda = \prod_{i=1}^{n} \sum_{j=1}^{n} |\sigma_i(\alpha_j)|$$

depending on K.

For any nonzero ideal $I \subset \mathcal{O}_K$, let $m \in \mathbb{N}$ such that $m^n \leq \mathrm{N}_K(I) = |\mathcal{O}_K/I| < (m+1)^n$.

Consider the following $(m+1)^n$ elements in $\mathcal{O}_K$ defiend by

$$\sum_{j=1}^{n} m_j \alpha_j$$

with $0 \leq m_j \leq m$.

By construction this is a larger set of elements than $\mathrm{N}_K(I)$, so two must be equal modulo I. Take the difference of those two elements, call it

$$\sum_{j=1}^{n} r_j \alpha_j \in I$$

with $|r_j| \leq m$, and call this element our α.

Then we have

$$|\mathrm{N}_{K/\mathbb{Q}}(\alpha)| = \left| \prod_{i=1}^{n} \sum_{j=1}^{n} r_j \sigma_i(\alpha_j) \right| \leq m^n \prod_{i=1}^{n} \sum_{j=1}^{n} |\sigma_i(\alpha_j)| \leq \lambda \, \mathrm{N}_K(I)$$

since $m_n \leq \mathrm{N}_K(I)$ by construction. □

Corollary 11.2.2. *Every ideal class of K contains an integral ideal $J \subset \mathcal{O}_K$ with $\mathrm{N}_K(J) \leq \lambda$, with λ as above.*

Proof. Given an ideal class $C \in \mathrm{Cl}(K) = I_K/P_K$, we know that C^{-1} exists since the class group is indeed a group. Fix any integral ideal $I \in C^{-1}$.

By the previous theorem there exists some nonzero $\alpha \in I$ such that

$$|\mathrm{N}_{K/\mathbb{Q}}(\alpha)| \leq \lambda \, \mathrm{N}_K(I).$$

Note that $(\alpha) \subset I \subset \mathcal{O}_K$, meaning that $(\alpha) = IJ$ for some $J \subset \mathcal{O}_K$.

Consider this equation modulo P_K, i.e. in I_K/P_K, we get $IJ \equiv 1 \pmod{P_K}$ since (α) is principal. Now I is a representative for the coset C^{-1} and J one for C, so $J \in C$.

Then

$$|\mathrm{N}_{K/\mathbb{Q}}(\alpha)| = \mathrm{N}((\alpha)) = \mathrm{N}(I)\,\mathrm{N}(J) \leq \lambda \, \mathrm{N}(I)$$

and so $\mathrm{N}(J) \leq \lambda$. □

Corollary 11.2.3. *The class number $h(K)$ is finite.*

Proof. There are only finitely many primes $p \in \mathbb{Z}$ such that $|p| < \lambda$, and above each of those there is a finite number of ideals J, whose norms are greater than the size of the prime they lie above, and so there are only finitely many ideals in $\mathcal{O}_K$ with norm less than λ.

Hence by the above corollary there are only finitely many ideal classes, since *each* ideal class contains an integral ideal with norm less than or equal to λ. □

Example 11.2.4. Let $K = \mathbb{Q}(\sqrt{2})$, so $\mathcal{O}_K = \mathbb{Z}[\sqrt{2}]$, with the integral basis $\{1, \sqrt{2}\}$. Then

$$\lambda = (1+\sqrt{2})(1+|-\sqrt{2}|) = (1+\sqrt{2})^2 \approx 5.8$$

so the only candidate primes we need consider are 2, 3, and 5.

Now $2\mathcal{O}_K = (\sqrt{2})^2$ factors, but $3\mathcal{O}_K$ and $5\mathcal{O}_K$ are prime ideals. For the latter two we must therefore have $e = 1$ and $f = 2$, and $\mathrm{N}(3\mathcal{O}_K) = 3^2 = 9$ along with $\mathrm{N}(5\mathcal{O}_K) = 5^2 = 25$, both of which exceed λ.

Hence the ideals in $\mathcal{O}_K$ with norms less than λ are $\mathcal{O}_K = (1)$, $\sqrt{2}\mathcal{O}_K = (\sqrt{2})$, and $2\mathcal{O}_K = (2)$, all of which are principal, so $\mathcal{O}_K$ is a principal ideal domain. ▲

Lecture 12 Minkowski's Theorem

12.1 Using Geometry to Improve λ

We showed last time that given a number field K, there exists some λ (depending on K) such that for every nonzero ideal $I \subset \mathcal{O}_K$ there is some nonzero $\alpha \in I$ for which

$$|\mathrm{N}_{K/\mathbb{Q}}(\alpha)| \leq \lambda \,\mathrm{N}_K(I).$$

Last time we showed that

$$\lambda = \prod_{i=1}^{n} \sum_{j=1}^{n} |\sigma_i(\alpha_j)|$$

works, where $\{\alpha_i\}$ is an integral basis for $\mathcal{O}_K$ and $\sigma_j \colon K \hookrightarrow \mathbb{C}$ are the embeddings of K into $\mathbb{C}$.

The choice of this λ, as we saw at the end last time, decides how many primes we need to study in order to tell if $\mathcal{O}_K$ is a principal ideal domain or not. It is therefore in our interest to sharpen λ, making it smaller.

Definition 12.1.1 (Lattice)**.** A ***lattice*** Λ in $V = \mathbb{R}^n$ is an additive subgroup of V of the form

$$\Lambda = \mathbb{Z}v_1 + \mathbb{Z}v_2 + \ldots + \mathbb{Z}v_n$$

with $v_1, v_2, \ldots, v_n$ linearly independent over $\mathbb{R}$.

Example 12.1.2. The standard lattice that comes to mind is the integer lattice, i.e. in $V = \mathbb{R}^2$ we have $\Lambda = \mathbb{Z}^2 = \mathbb{Z}e_1 + \mathbb{Z}e_2$, where $e_1 = (1,0)$ and $e_2 = (0,1)$. ▲

Let K be a number field of degree n, and let $\sigma_1, \sigma_2, \ldots, \sigma_r$ be the real embeddings of K, with $\tau_1, \overline{\tau_1}, \ldots, \tau_2, \overline{\tau_s}$ being the complex embeddings of K

Consider the following function $\varphi \colon K \to \mathbb{R}^n$ defined by

$$\varphi(\alpha) = (\sigma_1(\alpha), \sigma_2(\alpha), \ldots, \sigma_r(\alpha), \mathrm{Re}\,\tau_1(\alpha), \mathrm{Im}\,\tau_1(\alpha), \ldots, \mathrm{Re}\,\tau_s(\alpha), \mathrm{Im}\,\tau_s(\alpha)).$$

This is an additive homomorphism with $\ker\varphi = \{0\}$, and hence φ is an embedding.

Date: February 15th, 2018.

Proposition 12.1.3. *Let K be a number field with ring of integers $\mathcal{O}_K$. Then $\Lambda = \Lambda_{\mathcal{O}_K} = \varphi(\mathcal{O}_K)$ is a lattice in $\mathbb{R}^n$.*

Proof. Let $\alpha_1, \alpha_2, \ldots, \alpha_n$ be an integral basis for $\mathcal{O}_K$, and set $v_i = \varphi(\alpha_i)$ for $i = 1, 2, \ldots, n$.

Then

$$\Lambda = \mathbb{Z}v_1 + \mathbb{Z}v_2 + \ldots + \mathbb{Z}v_n,$$

since $\mathcal{O}_K = \mathbb{Z}\alpha_1 + \mathbb{Z}\alpha_2 + \ldots + \mathbb{Z}\alpha_n$.

We need to verify that v_i are linearly independent over $\mathbb{R}$, so let us compute the determinant of the matrix made up of them as rows. Let

$$\delta = \det \begin{bmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{bmatrix}$$

which expanded is

$$\begin{vmatrix} \sigma_1(\alpha_1) & \cdots & \sigma_r(\alpha_1) & \operatorname{Re}\tau_1(\alpha_1) & \operatorname{Im}\tau_1(\alpha_1) & \cdots & \operatorname{Re}\tau_s(\alpha_1) & \operatorname{Im}\tau_s(\alpha_1) \\ \vdots & & & & & & & \vdots \\ \sigma_1(\alpha_n) & \cdots & \sigma_r(\alpha_n) & \operatorname{Re}\tau_1(\alpha_n) & \operatorname{Im}\tau_1(\alpha_n) & \cdots & \operatorname{Re}\tau_s(\alpha_n) & \operatorname{Im}\tau_s(\alpha_n) \end{vmatrix}.$$

If we multiply the first Im column by i, and then add the Im-column to the Re-column, we get

$$\frac{1}{i}\begin{vmatrix} \sigma_1(\alpha_1) & \cdots & \sigma_r(\alpha_1) & \tau_1(\alpha_1) & i\operatorname{Im}\tau_1(\alpha_1) & \cdots & \operatorname{Re}\tau_s(\alpha_1) & \operatorname{Im}\tau_s(\alpha_1) \\ \vdots & & & & & & & \vdots \\ \sigma_1(\alpha_n) & \cdots & \sigma_r(\alpha_n) & \tau_1(\alpha_n) & i\operatorname{Im}\tau_1(\alpha_n) & \cdots & \operatorname{Re}\tau_s(\alpha_n) & \operatorname{Im}\tau_s(\alpha_n) \end{vmatrix}.$$

Next add -2 times the τ_1-column to the $i\,\mathrm{Im}$-column, whence we have

$$\frac{1}{-2i}\begin{vmatrix} \sigma_1(\alpha_1) & \cdots & \sigma_r(\alpha_1) & \tau_1(\alpha_1) & \overline{\tau_1}(\alpha_1) & \cdots & \operatorname{Re}\tau_s(\alpha_1) & \operatorname{Im}\tau_s(\alpha_1) \\ \vdots & & & & & & & \vdots \\ \sigma_1(\alpha_n) & \cdots & \sigma_r(\alpha_n) & \tau_1(\alpha_n) & \overline{\tau_1}(\alpha_n) & \cdots & \operatorname{Re}\tau_s(\alpha_n) & \operatorname{Im}\tau_s(\alpha_n) \end{vmatrix}.$$

Repeat this for tall the columns corresponding to complex embeddings to get

$$\frac{1}{(-2i)^s}\begin{vmatrix} \sigma_1(\alpha_1) & \cdots & \sigma_r(\alpha_1) & \tau_1(\alpha_1) & \overline{\tau_1}(\alpha_1) & \cdots & \tau_s(\alpha_1) & \overline{\tau_s}(\alpha_1) \\ \vdots & & & & & & & \vdots \\ \sigma_1(\alpha_n) & \cdots & \sigma_r(\alpha_n) & \tau_1(\alpha_n) & \overline{\tau_1}(\alpha_n) & \cdots & \tau_s(\alpha_n) & \overline{\tau_s}(\alpha_n) \end{vmatrix}.$$

But the determinant there is the discriminant of K, so

$$|\delta|^2 = \frac{1}{2^{2s}}|\operatorname{disc}(K)| \neq 0$$

and so $\delta \neq 0$, meaning that v_i are indeed linearly independent over $\mathbb{R}$. □

Definition 12.1.4 (Fundamental parallelotope)**.** A ***fundamental parallelotope*** for Λ is the set

$$D = \Big\{ \sum_{i=1}^{n} a_i v_i \;\Big|\; 0 \leq a_i < 1 \Big\}.$$

We denote $D = \mathbb{R}^n/\Lambda$.

Example 12.1.5. With $V = \mathbb{R}^2$ and $\Lambda = \mathbb{Z}^2$, the fundamental parallelotope is the unit square between $(0,0)$, $(1,0)$, $(1,1)$, and $(0,1)$, with the right and top edges excluded. ▲

Note that

$$V = \bigsqcup_{\lambda \in \Lambda} (\lambda + D)$$

meaning that shifted D tile the space V.

Proposition 12.1.6. *We have*

$$\operatorname{Vol}(\mathbb{R}^n/\Lambda) = \left|\det \begin{bmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{bmatrix}\right|$$

and $\operatorname{Vol}(\mathbb{R}^n/\Lambda)$ *is independent of the choice of* v_i.

These are elementary linear algebra considerations. The first one can in fact be taken as the definition of the determinant, and the second one follows from there being a transformation between any two integral bases whose determinant is ± 1.

Theorem 12.1.7. *The map* $\varphi\colon K \hookrightarrow \mathbb{R}^n$ *sends* $\mathcal{O}_K$ *to a lattice* $\Lambda = \varphi(\mathcal{O}_K)$ *with* $\operatorname{Vol}(\mathbb{R}^n/\Lambda) = 2^{-s}\sqrt{|\operatorname{disc}(K)|}$. *Moreover*

$$\varphi(K) = \mathbb{Q}v_1 + \mathbb{Q}v_2 + \ldots + \mathbb{Q}v_n$$

is dense in $\mathbb{R}^n$.

Let $V = \mathbb{R}^n$ and assume $\Lambda_1 \subset \Lambda_2 \subset V$ are lattices. Then Λ_2/Λ_1 is a finite group, and

$$\operatorname{Vol}(\mathbb{R}^n/\Lambda_1) = \operatorname{Vol}(\mathbb{R}^n/\Lambda_2) \cdot |\Lambda_2/\Lambda_1|.$$

Example 12.1.8. Consider $V = \mathbb{R}^2$ and $\Lambda_2 = \mathbb{Z} \times \mathbb{Z} \supset \Lambda_1 = 2\mathbb{Z} \times \mathbb{Z}$, i.e. in the second one we only have even integers in our x-coordinates. Then the volume of the first fundamental parallelotope is $1 \cdot 1 = 1$, and the second one is $2 \cdot 1 = 2$, and the factor between them of course is 2. ▲

We are now almost at the point where this excursion in geometry ties into our number theory:

Example 12.1.9. Let $\varphi\colon K \hookrightarrow \mathbb{R}^n$ be as before, and let $\Lambda = \varphi(\mathcal{O}_K)$ be the same lattice. Let $I \subset \mathcal{O}_K$ be an ideal.

Then $\Lambda_I = \varphi(I) \subset \Lambda$ is a sublattice, and so

$$\begin{aligned} \operatorname{Vol}(\mathbb{R}^n/\Lambda_I) &= \operatorname{Vol}(\mathbb{R}^n/\Lambda) \cdot |\mathcal{O}_K/I| = \operatorname{Vol}(\mathbb{R}^n/\Lambda)\, \mathrm{N}_K(I) \\ &= \frac{1}{2^s}\sqrt{|\operatorname{disc}(K)|}\, \mathrm{N}_K(I). \end{aligned}$$ ▲

Let us now define a special norm on $\mathbb{R}^n$ depending on K, a number field of degree n with r real embeddings and $2s$ complex embeddings. For $x = (x_1, \ldots, x_r, x_{r+1}, \ldots, r_n) \in \mathbb{R}^n$ we define

$$\mathrm{N}(x) = x_1 x_2 \cdots x_r (x_{r+1}^2 + x_{r+2}^2)(x_{r+3}^2 + x_{r+4}^2) \cdots (x_{n-1}^2 + x_n^2)$$

which is of note since if $\varphi\colon K \hookrightarrow \mathbb{R}^n$ by $\alpha \mapsto \varphi(\alpha) = x$, then $\mathrm{N}_{K/\mathbb{Q}}(\alpha) = \mathrm{N}(x)$ since

$$\mathrm{N}_{K/\mathbb{Q}}(\alpha) = \prod_{i=1}^{r} \sigma_i(\alpha) \prod_{j=1}^{s} \tau_j(\alpha)\overline{\tau_j}(\alpha).$$

Note that whilst we defined this in terms of a number field K, we could equally well forget about the number field and define such a norm on $\mathbb{R}^n$ for any partition $n = r + 2s$.

Theorem 12.1.10 (Minkowski)**.** *Let $n = r + 2s$, $r, s \in \mathbb{Z}$. For any lattice $\Lambda \subset \mathbb{R}^n$ there exists a nonzero $x \in \Lambda$ such that*

$$|\mathrm{N}(x)| \leq \frac{n!}{n^n}\Big(\frac{8}{\pi}\Big)^s \operatorname{Vol}(\mathbb{R}^n/\Lambda).$$

Notice the complete lack of number fields above. It works for any partition $n = r + 2s$; it's pure analysis.

Theorem 12.1.11. *For every nonzero ideal $I \subset \mathcal{O}_K$, there exists a nonzero $\alpha \in I$ such that*

$$|\mathrm{N}_{K/\mathbb{Q}}(\alpha)| \leq \frac{n!}{n^n}\Big(\frac{4}{\pi}\Big)^s \sqrt{|\mathrm{disc}(K)|}\,\mathrm{N}_K(I).$$

Proof. Simply apply Minkowski's theorem to $\Lambda_I = \varphi(I)$. □

In other words we can use

$$\lambda = \frac{n!}{n^n}\Big(\frac{4}{\pi}\Big)^s \sqrt{|\mathrm{disc}(K)|}$$

in the type of considerations made last time:

Corollary 12.1.12. *Every ideal class of K contains an integral ideal $J \subset \mathcal{O}_K$ with*

$$\mathrm{N}_K(J) \leq \frac{n!}{n^n}\Big(\frac{4}{\pi}\Big)^s \sqrt{|\mathrm{disc}(K)|}.$$

Remark 12.1.13. The quantity

$$\frac{n!}{n^n}\Big(\frac{4}{\pi}\Big)^s$$

is called the ***Minkowski constant*** and notably decays very, very quickly, meaning that for number fields of fixed discriminant, as $n \to \infty$ almost all of them are principal ideal domains.

Example 12.1.14. Let $K = \mathbb{Q}(\xi_5)$ with $\mathcal{O}_K = \mathbb{Z}[\xi_5]$ and $[K : \mathbb{Q}] = \varphi(5) = 4 = n$. We have $\mathrm{disc}(K) = 5^{5-2} = 125$ since $s = 2$, and so

$$\mathrm{N}_K(J) \leq \frac{4!}{4^4}\Big(\frac{4}{\pi}\Big)^2 \sqrt{125} < 2$$

and therefore $\mathrm{N}_K(J) = 1$, so $J = \mathcal{O}_K$, meaning that every ideal class contains $\mathcal{O}_K$, and therefore $\mathcal{O}_K$ is a principal ideal domain. ▲

Let us repeat the computation from last time as well, to show how much better this λ is.

Example 12.1.15. Let $K = \mathbb{Q}(\sqrt{2})$, so $s = 0$ and $n = 2$, and $\operatorname{disc}(K) = 4 \cdot 2 = 8$. Then

$$\mathrm{N}_K(J) \leq \frac{2!}{2^2}\Big(\frac{4}{\pi}\Big)^0 \sqrt{8} = \sqrt{2},$$

so $\mathrm{N}_K(J) = 1$, and $\mathcal{O}_K$ is a principal ideal domain. Notice how this time we didn't have to try to factor a single prime ideal in $\mathcal{O}_K$. ▲

Corollary 12.1.16. *For $K \neq \mathbb{Q}$, i.e. $[K : \mathbb{Q}] > 1$, we have $|\operatorname{disc}(K)| > 1$.*

Proof. Simyply use the last corollary. Since $\mathrm{N}_K(J) \geq 1$, we have

$$1 \leq \frac{n!}{n^n}\Big(\frac{4}{\pi}\Big)^s \sqrt{|\operatorname{disc}(K)|}$$

which rearranged becomes

$$\sqrt{|\operatorname{disc}(K)|} \geq \frac{n^n}{n!}\Big(\frac{\pi}{4}\Big)^s > 1$$

for every $n > 1$. □

It remains to prove Minkowski's theorem. This will take some work, but first:

Lemma 12.1.17. *Let $\Lambda \subset \mathbb{R}^n$ be a lattice. Let E be a convex, measurable, symmetric subset of $\mathbb{R}^n$. If $\operatorname{Vol}(E) > 2^n \operatorname{Vol}(\mathbb{R}^n/\Lambda)$, then E contains a nonzero element of Λ.*

Moreover if E is also compact, then the assumption can be weakened to $\operatorname{Vol}(E) \geq 2^n \operatorname{Vol}(\mathbb{R}^n/\Lambda)$.

Before we prove this, let us first recall what the various properties above mean. We call a set ***convex*** if for every $x, y \in E$ we also have $ax + (1-a)y \in E$ for every $0 \leq a \leq 1$, i.e. the line segment between any two points in the set is also contained in the set.

By ***measurable*** we mean a Lebesgue measurable set, so it is in the σ-algebra generated by the opens sets in $\mathbb{R}^n$.

When we say ***symmetric*** we mean that if $x \in E$ then $-x \in E$ as well.

Lecture 13 Toward Minkowski's Theorem

13.1 Proving Minkowski's Theorem

We'll start by proving the lemma stated at the end of last lecture.

Proof. Let $F = \mathbb{R}^n/\Lambda$ be the fundamental parallelotope for Λ. Then

$$\mathbb{R}^n = \bigsqcup_{x \in \Lambda} x + F$$

meaning that

$$\frac{1}{2}E = \bigsqcup_{x \in \Lambda} \Big(\frac{1}{2}E \cap (x + F)\Big).$$

Date: February 20th, 2018.

By assumption,

$$\operatorname{Vol}(F) < \frac{1}{2^n}\operatorname{Vol}(E) = \operatorname{Vol}(1/2E) = \sum_{x\in\Lambda}\operatorname{Vol}(1/2E\cap(x+F)) = \sum_{x\in\Lambda}\operatorname{Vol}((1/2E-x)\cap F)$$

since the Lebesgue measure is translation invariant. Hence $(1/2E-x)\cap(1/2E-y)\neq\varnothing$ for some $x,y\in\Lambda$, $x\neq y$, since otherwise the volume would be less than or equal to $\operatorname{Vol}(F)$, which is a contradiction.

So $1/2e_1 - x = 1/2e_2 - y$ for some $e_1, e_2 \in E$, meaning that

$$x - y = \frac{1}{2}e_1 - \frac{1}{2}e_2 = \frac{1}{2}(e_1 + (-e_2)) \in E$$

since E is symmetric, so $-e_2 \in E$, and E is convex, with the last step above being a convex combination of e_1 and $-e_2$. Moreover $x - y \in \Lambda$ since Λ is a group, whence $x - y \neq 0$ is in $\Lambda \cap E$.

Suppose now that E is compact and $\operatorname{Vol}(E) \geq 2^n \operatorname{Vol}(\mathbb{R}^n/\Lambda)$. For $m = 1, 2, \ldots$, we have

$$\operatorname{Vol}((1+1/m)E) = (1+1/m)^n \operatorname{Vol}(E) > 2^n \operatorname{Vol}(\mathbb{R}^n/\Lambda),$$

so by the above there exists some nonzero $x_m \in \Lambda \cap (1+1/m)E$.

Hence $\{ x_m \}_{m=1}^{\infty} \subset \Lambda \cap (2E)$, where $2E$ is compact (it's closed and bounded in $\mathbb{R}^n$), and $\Lambda \cap (2E)$ is finite since Λ is discrete. Hence $\{ x_m \}$ takes finitely many values, meaning that there exists some subsequence $\{ x_k \}$ with $x_k = x$ for all k. Therefore $x = x_k \in (1+1/k)E$ for all k, so when in the limit $(1+1/k)E$ goes to $\overline{E} = E$ since E is compact. Hence $x \in E \cap \Lambda$. □

Corollary 13.1.1. *Let A be a compact, convex, symmetric subset of $\mathbb{R}^n$ with $\operatorname{Vol}(A) > 0$ and $|\mathrm{N}(a)| \leq 1$ for all $a \in A$, where by N we mean the special norm on $\mathbb{R}^n$ defined by $n = r + 2s$ as before.*

Then for every lattive $\Lambda \subset \mathbb{R}^n$ there exists some nonzero $x \in \Lambda$ with

$$|\mathrm{N}(x)| \leq \frac{2^n}{\operatorname{Vol}(A)} \operatorname{Vol}(\mathbb{R}^n/\Lambda).$$

Proof. Let $E = tA$ where

$$t^n = \frac{2^n}{\operatorname{Vol}(A)} \operatorname{Vol}(\mathbb{R}^n/\Lambda).$$

Then

$$\operatorname{Vol}(E) = \operatorname{Vol}(tA) = t^n \operatorname{Vol}(A) = 2^n \operatorname{Vol}(\mathbb{R}^n/\Lambda).$$

By the lemma, there exists a nonzero $x \in \Lambda \cap E$ such that $x = ta$ for some $a \in A$. Then

$$|\mathrm{N}(x)| = |\mathrm{N}(ta)| = |t^n \mathrm{N}(a)| \leq \frac{2^n}{\operatorname{Vol}(A)} \operatorname{Vol}(\mathbb{R}^n/\Lambda).$$ □

Theorem 13.1.2 (Minkowski)**.** *For every lattice $\Lambda \subset \mathbb{R}^n$ there exists a nonzero $x \in \Lambda$ such that*

$$|\mathrm{N}(x)| \leq \frac{n!}{n^n}\Big(\frac{8}{\pi}\Big)^s \operatorname{Vol}(\mathbb{R}^n/\Lambda)$$

where $n = r + 2s$.

Proof. Define the set A by

$$|x_1| + |x_2| + \ldots + |x_r| + 2(\sqrt{x_{r+1}^2 + x_{r+2}^2} + \ldots + \sqrt{x_{n-1}^2 + x_n^2}) \leq n,$$

where $n = r + 2s$. Then A is compact (it's certainly closed and bounded), it is convex (it suffices to study the middle points between any two points), and it's trivially symmetric. We also have $\mathrm{Vol}(A) > 0$ since we at the very least contain, say, some small intervals in each coordinate.

Moreover for $a \in A$ we ahve $|\mathrm{N}(a)| \leq 1$ since by the AM-GM inequality

$$\begin{aligned} 1 &\geq \frac{|x_1| + |x_2| + \ldots + |x_r| + 2(\sqrt{x_{r+1}^2 + x_{r+2}^2} + \ldots + \sqrt{x_{n-1}^2 + x_n^2})}{n} \\ &\geq (|x_1||x_2| \cdots |x_r|(x_{r+1}^2 + x_{r+2}^2) \cdots (x_{n-1}^2 + x_n^2))^{1/n} = \mathrm{N}(a)^{1/n}. \end{aligned}$$

We now claim

$$\mathrm{Vol}(A) = \frac{n^n}{n!} 2^r \left(\frac{\pi}{2}\right)^s.$$

Then the theorem follows from the corollary above.

Let $V_{r,s}(t)$ be the volume of the subset of $\mathbb{R}^{r+2s}$ defined by

$$|x_1| + |x_2| + \ldots + |x_r| + 2(\sqrt{x_{r+1}^2 + x_{r+2}^2} + \ldots + \sqrt{x_{n-1}^2 + x_n^2}) \leq t.$$

Then $\mathrm{Vol}(A) = V_{r,s}(n)$ and by scaling $V_{r,s}(t) = t^{r+2s} V_{r,s}(1)$. We will show that

$$V_{r,2}(1) = \frac{1}{(r+2s)!} 2^r \left(\frac{\pi}{2}\right)^s.$$

Now if $r > 0$, we have could move $|x_r|$ to the right-hand side and then bound by $1 - t$, so

$$\begin{aligned} V_{r,s}(1) &= 2 \int_0^1 V_{r-1,s}(1-t)\, dt = 2 \int_0^1 (1-t)^{r-1+2s} V_{r-1,s}(1)\, dt \\ &= \frac{2}{r+2s} V_{r-1,s}(1), \end{aligned}$$

which by induction becomes

$$V_{r,s}(1) = \frac{2^r}{(r+2s)(r+2s-1)\cdots(2s+1)} V_{0,s}(1).$$

Note that if $s = 0$ we define $V_{0,0}(1) = 1$ (since $V_{1,0}(1) = 2 = 2V_{0,0}(1)$), and we are done.

Now if $s > 0$, $V_{0,s}(1)$ is given by

$$2(\sqrt{x_{r+1}^2 + x_{r+2}^2} + \ldots + \sqrt{x_{n-1}^2 + x_n^2}) \leq 1,$$

which if we move one of the square roots over yields

$$V_{0,s}(1) = \iint_R V_{0,s-1}(1 - 2\sqrt{x^2 + y^2})\, dx\, dy$$

where $R = \{\, x^2 + y^2 \le 1/4 \,\}$ is the circle of radius $1/2$. We therefore switch to polar coordinates, $x = \rho\cos(\theta)$ and $y = \rho\sin(\theta)$, with $dx\,dy = \rho\,d\rho\,d\theta$, whence our integral becomes

$$\begin{aligned} V_{0,s}(1) &= \int_0^{2\pi}\int_0^{1/2} V_{0,s-1}(1-2\rho)\rho\,d\rho\,d\theta \\ &= \int_0^{2\pi}\int_0^{1/2} (1-2\rho)^{2(s-1)} V_{0,s-1}(1)\rho\,d\rho\,d\theta \\ &= \frac{\pi}{2}\frac{1}{(2s)(2s-1)} V_{0,s-1}(1), \end{aligned}$$

so by induction

$$V_{0,s}(1) = \Big(\frac{\pi}{2}\Big)^s \frac{1}{(2s)(2s-1)\cdots 2\cdot 1} V_{0,0}(1)$$

whence

$$V_{r,s}(1) = \frac{1}{(r+2s)!} 2^r \Big(\frac{\pi}{2}\Big)^s. \qquad \square$$

13.2 The Dirichlet Unit Theorem

Let K be a number field and $\mathcal{O}_K$ its ring of integers. Let $\mathcal{O}_K^\times$ be the set of units in $\mathcal{O}_K$.

Next let $\sigma_1, \sigma_2, \ldots, \sigma_r$ be the real embeddins of K and $\tau_1, \tau_2, \ldots, \tau_s$ be the distinct nonconjugate compled embeddings of K, with $n = r + 2s$.

Define a logarithm map $\log\colon K^\times \to \mathbb{R}^{r+2}$ by

$$\log(\alpha) = \big(\log|\sigma_1(\alpha)|, \log|\sigma_2(\alpha)|, \ldots, \log|\sigma_r(\alpha)|, 2\log|\tau_1(\alpha)|, \ldots, 2\log|\tau_s(\alpha)|\big).$$

It is easy to check $\log(\alpha\beta) = \log(\alpha) + \log(\beta)$, making it a multiplicative-additive group homomorphism.

Therefore $\log(\mathcal{O}_K^\times)$ is an additive subgroup of $\mathbb{R}^{r+s}$. For $\alpha \in \mathcal{O}_K^\times$, we have

$$1 = |\mathrm{N}_{K/\mathbb{Q}}(\alpha)| = |\sigma_1(\alpha)\sigma_2(\alpha)\cdots\sigma_r(\alpha)|\tau_1(\alpha)|^2\cdots|\tau_s(\alpha)|^2|,$$

means that

$$0 = \log|\sigma_1(\alpha)| + \cdots + \log|\sigma_r(\alpha)| + 2\log|\tau_1(\alpha)| + \ldots + 2\log|\tau_s(\alpha)|$$

which means that

$$\log(\mathcal{O}_K^\times) \subset H = \{\, x \in \mathbb{R}^{r+s} \mid x_1 + x_2 + \ldots + x_{r+s} = 0 \,\},$$

a hyperplane with $\dim_{\mathbb{R}} H = r + s - 1$.

Proposition 13.2.1. *Consider* $\log|_{\mathcal{O}_K^\times}$*, by which we mean the logarithm restricted to* $\mathcal{O}_K^\times$*. Then*

(*i*) $\ker(\log) = \mu(K)$ *is the group of roots of unity in* K*, which is finite.*

(*ii*) $\mathrm{Im}(\log)$ *is a lattice in* H*. Hence* $\mathrm{Im}(\log) \cong \mathbb{Z}^{r+s-1}$.

Corollary 13.2.2 (Dirichlet unit theorem)**.** *We have* $\mathcal{O}_K^\times \cong \mu(K) \times \mathbb{Z}^{r+s-1}$.

To prove these, we first need the following lemma.

Lemma 13.2.3. *The number of elements on* $\mathcal{O}_K$ *with bounded embeddings is finite, i.e.*

$$\#\{\, \alpha \in \mathcal{O}_K \mid |\sigma_i(\alpha)| < M, |\tau_j(\alpha)| < M, i = 1, 2, \ldots, r, j = 1, 2, \ldots, s \,\}$$

is finite for every $M > 0$.

Proof. Note that $\alpha \in \mathcal{O}_K$ is a root of a monic polynomial in $\mathbb{Z}[x]$ of degree less than or equal to n, with coefficients bounded by

$$\max_{1 \le i \le n} \binom{n}{i} M^i$$

by the binomial theorem. There exists only finitely many such polynomials, and therefore only finitely many such roots. □

Lecture 14 Dirichlet Unit Theorem

14.1 Dirichlet Unit Theorem

We start by proving the proposition stated last time.

Proof. The first part, that $\mu(K) \subset \ker(\log)$, is trivial, since roots of unity have absolute value 1, so the constituent logarithms all become 0.

For the opposite inclusion, $\ker(\log) \subset \mu(K)$, consider

$$\ker(\log) = \{\, \alpha \in \mathcal{O}_K^\times \mid |\sigma_i(\alpha)| = 1, |\tau_j(\alpha)| = 1, i = 1, 2, \ldots, r,\ j = 1, 2, \ldots, s \,\}.$$

By the lemma this is finite, i.e. $\#\ker(\log) < \infty$. So if we pick some $\alpha \in \ker(\log)$, the set $\{\, \alpha, \alpha^2, \alpha^3, \ldots \}$ must be finite—all of these elements are in the kernel, since log is a homomorphism. Hence $\alpha^m = \alpha^h$ for some $m > h$, so $\alpha^{m-h} = 1$, whence α is a root of unity, meaning that $\alpha \in \mu(K)$.

For the second part we need to show that $\log(\mathcal{O}_K^\times)$ is discrete, and that $\log(\mathcal{O}_K^\times)$ spans H over $\mathbb{R}$.

For any bounded set in H, it is contained in $A = [-M, M]^{r+s} \cap H$ for some M. Now the pre-image $\log^{-1}(A)$ in $\mathcal{O}_K$ is contained in

$$\{\, \alpha \in \mathcal{O}_K \mid |\sigma_i(\alpha)| < e^M, |\tau_j(\alpha)| < e^{M/2}, i = 1, 2, \ldots, r,\ j = 1, 2, \ldots, s \,\}$$

which by the lemma is finite. Hence $\log(\mathcal{O}_K^\times) \cap A$ is a finite set, and so $\log(\mathcal{O}_K^\times)$ is discrete.

To prove the second part we need two lemmata.

Lemma 14.1.1. *Fix any* k, $1 \le k \le r + s$. *For each* $\alpha \in \mathcal{O}_K$, *there exists some nonzero* $\beta \in \mathcal{O}_K$ *depending on* α *such that*

$$|\mathrm{N}_{K/\mathbb{Q}}(\beta)| \le \left(\frac{2}{\pi}\right)^s \sqrt{|\mathrm{disc}(K)|}$$

Date: February 22nd, 2018.

independent of α, and if

$$\log(\alpha) = (a_1, a_2, \dots, a_{r+s}) \qquad \textit{and} \qquad \log(\beta) = (b_1, b_2, \dots, b_{r+1})$$

then $b_i < a_i$ for all $i \neq k$.

Proof. Take E as the subset defined by $|x_i| \leq c_i$ for $i = 1, 2, \dots, r$, and $x_{r+1}^2 + x_{r+2}^2 \leq c_{r+1}, \dots, x_{n-1}^2 + x_n^2 \leq c_{r+s}$, where c_i are chosen to satisfy $0 < c_i < e^{a_i}$ for all $i \neq k$, and moreover

$$c_1 c_2 \cdots c_{r+s} = \left(\frac{2}{\pi}\right)^s \sqrt{|\mathrm{disc}(K)|},$$

which then gives us c_k.

Then

$$\mathrm{Vol}(E) = 2^r \pi^s c_1 c_2 \cdots c_{r+s} = 2^n \,\mathrm{Vol}(\mathbb{R}^n / \Lambda_{\mathcal{O}_K}),$$

where we know $\mathrm{Vol}(\mathbb{R}^n / \Lambda_{\mathcal{O}_K}) = 2^{-s}\sqrt{|\mathrm{disc}(K)|}$.

This set E is convex, compact, symmetric, and Lebesgue measurable, so we can apply Minkowski's theorem, saying that there exists a nonzero $x \in E \cap \Lambda_{\mathcal{O}_K}$. Now take $\beta \in \mathcal{O}_K$ such that $\varphi(\beta) = x$, where $\varphi \colon \mathcal{O}_K \hookrightarrow \mathbb{R}^n \cap E$ simply sends β a vector with each component being an embedding of β.

Then

$$|\mathrm{N}_{K/\mathbb{Q}}(\beta)| = |\mathrm{N}(x)| \leq \left(\frac{2}{\pi}\right)^s \sqrt{|\mathrm{disc}(K)|}$$

and β satisfies pur requirements by the choice of c_i. □

Lemma 14.1.2. *Fix any k, $1 \leq k \leq r+s$. Then there exists a unit $u \in \mathcal{O}_K^\times$ such that if*

$$\log(u) = (y_1, y_2, \dots, y_{r+s}),$$

then $y_i < 0$ for all $i \neq k$ and $y_k > 0$ (they couldn't all be negative, since their sum must be 0).

Proof. Take any $\alpha_1 \neq 0$ in $\mathcal{O}_K$ and apply the last lemma repeatedly to construct α_2, then α_3, and so forth. Thus for each $i \neq k$ the ith coordinate of $\log(\alpha_{j+1})$ is less than the ith coordinate of $\log(\alpha_j)$.

Now since

$$\mathrm{N}_K((\alpha_j)) = |\mathrm{N}_{K/\mathbb{Q}}(\alpha_j)| \leq \left(\frac{2}{\pi}\right)^s \sqrt{|\mathrm{disc}(K)|}$$

if a uniform bound, and since there exists only finitely many distinct ideals of bounded norm (since they all lie above a finite number of primes less than some bound), we must have $(\alpha_j) = (\alpha_h)$ for some $j < h$, and so $\alpha_j = u\alpha_j$ for some unit $u \in \mathcal{O}_K^\times$.

Hence

$$\log(\alpha_h) = \log(u\alpha_j) = \log(u) + \log(\alpha_j).$$

Call the ith coordinate of the left-hand side $a_{h,i}$ and the ith coordinates of the two addends in the right-hand side y_i and $a_{j,i}$ respectively. Then for $j < h$ we have $a_{h,i} = y_i + a_{j,i}$ for $i \neq k$, and so $a_{h,i} < a_{j,i}$ meaning that $y_i < 0$ for every $i \neq k$. □

With this in hand we apply the second lemma for each $1 \leq k \leq r+s-1$ to obtain $u_1, u_2, \ldots, u_{r+s-1} \in \mathcal{O}_K^\times$, where $\log(u_j)$ has positive jth coordinate and all other coordinates negative.

Set $v_i = \log(u_i) = (y_{i,1}, y_{i,2}, \ldots, y_{i,r+s-1})$, so $v_{i,j} < 0$ if $i \neq j$ and $y_{i,i} > 0$.

We claim that the set $\{ v_1, v_2, \ldots, v_{r+s-1} \}$ spans H over $\mathbb{R}$. In other words we want to show that it is a linearly independent set, since the dimension of H over $\mathbb{R}$ is exactly $r+s-1$.

Suppose

$$t_1 w_1 + t_2 w_2 + \ldots + t_{r+s-1} w_{r+s-1} = 0$$

for $t_i \in \mathbb{R}$, not all $t_i = 0$, where w_i are the columns of the matrix whose rows are v_i. We may assume $t_k = 1$ for some k, and $|t_i| \leq 1$ for $i \neq k$ (simply find the largest coefficient and divide both sides by it).

Then the kth coordinate is

$$0 = \sum_{i=1}^{r+s-1} t_i y_{i,k} = y_{k,k} + \sum_{i \neq k} t_i y_{i,k}$$

where $y_{k,k} > 0$ and $y_{i,k} < 0$. Note that at least one $t_j \neq 0$ for some $j \neq k$ since otherwise we'd have $0 = y_{k,k} > 0$, which is impossible.

Hence

$$0 > y_{k,k} + \sum_{i \neq k} y_{i,k} = 0$$

since $\log(v_i) \in H$. Hence v_i are linearly independent, and there are as many of them as there are dimensions in H, so they span H. □

14.2 Fermat's Last Theorem

Theorem 14.2.1 (Fermat's last theorem)**.** *Let $n \geq 3$ be an integer. Then $x^n + y^n = z^n$ has no nontrivial solutions in $\mathbb{Z}$ (nontrivial meaning $xyz \neq 0$).*

There is a direct reduction to be made by considering primes $p \mid n$, since if $n = pm$, then

$$(x^m)^p + (y^m)^p = (z^m)^p.$$

Hence if $x^n + y^n = z^n$ has a nontrivial solution, then $x^p + y^p = z^p$ also has a nontrivial solution.

Hence by contrapositive for any off prime p, $x^p + y^p = z^p$ having no nontrivial solutions implies that Fermat's last theorem is true.

Now assume $\gcd(x, y, z) = 1$ (otherwise factor the gcd out). We have two cases:

First, $p \nmid xyz$, and secondly p divides exactly one of x, y, and z.

For the second case, if $p \mid x$, then $y^p \equiv z^p \pmod{p}$, and so $y \equiv z \pmod{p}$, so if $p \mid x$ and $p \mid y$, then $\gcd(x, y, z) > 1$.

The first case is provided a partial answer by Kummer's theorem, namely with $p \nmid h(K)$, for $K = \mathbb{Q}(\zeta_p)$.

Lecture 15 Kummer's Theorem

15.1 Using the Dirichlet Unit Theorem

The Dirichlet unit theorem says that $\mathcal{O}_K^\times \cong \mu(K) \times \mathbb{Z}^{r+s-1}$, which in turn is isomorphic to $\mathbb{Z}/\omega\mathbb{Z} \times \mathbb{Z}^{r+s-1}$, where $|\mu(K)| = \omega$.

We call $\mathbb{Z}/\omega\mathbb{Z}$ the torsion part and $\mathbb{Z}^{r+s-1}$ the free part.

For any $u \in \mathcal{O}_K^\times$, we therefore have $u = \xi\varepsilon_1^{n_1}\varepsilon_2^{n_2}\cdots\varepsilon_{r+s-1}^{n_{r+s-1}}$, where $\xi \in \mu(K)$ and n_i, with $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{r+s-1}$ being free generators.

Then $\{\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{r+s-1}\}$ is called a ***fundamental system of units***.

Example 15.1.1. Let $K = \mathbb{Q}(\sqrt{D})$ with D being square free. We have two cases:

First, $D < 0$. We know that $\mathcal{O}_K^\times$ is $\{\pm 1, \pm i\}$ if $D = -1$, it's $\{\pm 1, \pm\xi_3, \pm\xi_3^2\}$ is $D = -3$, and it's $\{\pm 1\}$ otherwise.

We have $n = 2$, $r = 0$, and $s = 1$, so $r+s-1 = 0$, i.e. rank 0, so $\mathcal{O}_K^\times \cong \mu(K)$.

Next consider $D > 0$. Then $n = 2$, $r = 2$, and $s = 0$, so $r + s - 1 = 1$. We have $\mu(K) = \{\pm 1\}$, and so $\mathcal{O}_K^\times \cong \{\pm 1\} \times \mathbb{Z}$.

Let ε be a fundamental unit of K with $\varepsilon > 1$. Then $\varepsilon = a + b\sqrt{D}$ if $D \not\equiv 1 \pmod 4$ (and similar but with half integers for $D \equiv 1 \pmod 4$).

Then $\mathrm{N}(\varepsilon) = a^2 - b^2 D = \pm 1$, and ε is a fundamental solution of this equation since all units $u = \pm\varepsilon^m$ for some $m \in \mathbb{Z}$. This equation is known as ***Pell's equation***. ▲

15.2 Kummer's Theorem

Theorem 15.2.1 (Kummer's theorem)**.** *Suppose $p > 2$ is prime. If $p \nmid h(K)$, with $K = \mathbb{Q}(\xi_p)$, then there are no nontrivial solutions to $x^p + y^p = z^p$ with $p \nmid xyz$.*

Remark 15.2.2. A prime p satisfying the above is called a ***regular prime***, so this theorem says that Fermat's last theorem is true for all regular primes.

Before we proceed we recall some properties of the cyclotomic field $K = \mathbb{Q}(\xi_p)$.

1. $\mathcal{O}_K = \mathbb{Z}[\xi_p]$, and $(1 - \xi_p)\mathcal{O}_K$ is a prime ideal.
2. $(1 - \xi_p)^n = (1 - \xi_p)^{p-1} = p\mathcal{O}_K$, so p is totally ramified—this is what implies that $(1 - \xi_p)\mathcal{O})K$ is prime.
3. $\mathrm{N}_{K/\mathbb{Q}}(1 - \xi_p) = \pm p$.
4. $\mathbb{Z}/p\mathbb{Z} \cong \mathcal{O}_K/(1 - \xi_p)$ since $f = 1$.
5. $\mu(K) = \{\pm\xi_p^s\}_{0 \le s \le p-1}$.

In order to prove Kummer's theorem, we first need the following lemma.

Lemma 15.2.3. *(i) For each $\alpha \in \mathcal{O}_K$, there exists some $a \in \mathbb{Z}$ such that $\alpha^p \equiv a^p \pmod{(1 - \xi_p)^p}$.*

(ii) Every unit $\varepsilon \in \mathcal{O}_K^\times$ is of the form $\varepsilon = u \cdot \xi_p^r$ with $u \in \mathbb{R}$ and $r \in \mathbb{Z}$.

Date: February 27th, 2018.

Proof. (i) By the fourth property above, there exists some $a \in \mathbb{Z}$ such that $\alpha = a + (1-\xi_p)\beta$ for $\beta \in \mathcal{O}_K$, so

$$\alpha^p = a^p + \sum_{n=1}^{p-1} \binom{p}{n} a^n ((1-\xi_p)\beta)^{p-n} + (1-\xi_p)^p \beta^p.$$

Since $p \mid \binom{p}{n}$ for $1 \leq n \leq p$, and each such p has $p-1$ factors of $(1-\xi_p)$ by the second property, and the last coming from $(1-\xi_p)$, we have that the sum in the middle vanishes modulo $(1-\xi_p)^p$, as, of course, does the last term.

Hence $\alpha^p \equiv a^p \pmod{(1-\xi_p)^p}$.

(ii) Let $\varepsilon \in \mathcal{O}_K^\times \subset \mathbb{Z}[\xi_p]$. Thus $\varepsilon = f(\xi_p)$ for some $f(x) \in \mathbb{Z}[x]$.

For each $i \leq n \leq p-1$, let $\varepsilon_n = f(\xi_p^n) \in \mathcal{O}_K$, calling $\varepsilon = \varepsilon_1$.

Since ξ_p^n is a Galois conjugate of ξ_p, this ε_n is a Galois conjugate of ε, since embeddings are homomorphisms, and so $\varepsilon_n \in \mathcal{O}_K^\times$.

Note that the complex conjugate $\overline{\varepsilon_n}$ is precisely $\overline{\varepsilon_n} = \varepsilon_{p-n}$ since $\overline{\xi_p^n} = \xi_p^{-n} = \xi_p^{p-n}$.

Therefore $\varepsilon_n/\varepsilon_{p-n} \in \mathcal{O}_K^\times$, and $|\varepsilon_n/\varepsilon_{p-n}| = 1$, the Galois conjugates of which are $\varepsilon_m/\varepsilon_{p-m}$.

Hence the roots of the minimal polynomial of $\varepsilon_n/\varepsilon_{p-n}$ over $\mathbb{Q}$ all have absolute value 1, and therefore they must be pth roots of unity.

So $\varepsilon/\varepsilon_{p-1} = \pm\xi_p^s$ for some s. Since p is an odd prime, $\gcd(p,2) = 1$, and so we can find some r such that $s \equiv 2r \pmod{p}$, whence we can write this in turn as $\pm\xi_p^{2r}$.

Now by the fourth property there exists some a such that $\varepsilon \equiv a \pmod{(1-\xi_p)}$, and taking complex conjugates we get $\overline{\varepsilon} = \varepsilon_{p-1} \equiv a \pmod{(1-\xi_p)}$. Strictly speaking we should conjugate the ideal in the modulus too, but we have shown before that we get the same ideal.

Hence $\varepsilon \equiv \overline{\varepsilon} \pmod{(1-\xi_p)}$, and we can write

$$\varepsilon_{p-1} \equiv \varepsilon \equiv \pm\xi_p^{2r}\varepsilon_{p-1} \equiv \pm\varepsilon_{p-1} \pmod{(1-\xi_p)}$$

since $\xi_p^{2r} \equiv 1 \pmod{(1-\xi_p)}$.

Let us now decide whether $\pm$ should be positive or negative. Suppose $\varepsilon_{p-1} \equiv -\varepsilon_{p-1} \pmod{(1-\xi_p)}$. This implies $2\varepsilon_{p-1} \equiv 0 \pmod{(1-\xi_p)}$.

Taking norms we get $\mathrm{N}(1-\xi_p) \mid \mathrm{N}(2\varepsilon_{p-1})$, so $\pm p \mid \pm 2^{p-1}$, which is a contadiction.

So we must have $\varepsilon/\varepsilon_{p-1} = \xi_p^{2r}$.

Hence $\varepsilon\xi_p^{-r} = \varepsilon_{p-1}\xi_p^r = \overline{\varepsilon\xi_p^{-r}}$, so $\varepsilon\xi_p^{-r}$ is its own complex conjugate, ergo real, so $\varepsilon\xi_p^{-r} = u \in \mathbb{R}$ and hence $\varepsilon = u\xi_p^r$. □

Proof of Kummer's theorem. We should assume $x \not\equiv y \pmod{p}$. To see why, suppose $x \equiv y \equiv -z \pmod{p}$. Then $x^p + y^p = z^p$ implies $-z + (-z) \equiv z \pmod{p}$, so $3z \equiv 0 \pmod{p}$. But $p \nmid xyz$, so $p \mid 3$, and this is a contradiction for $p \neq 3$.

Secondly, suppose $x \equiv y \not\equiv -z \pmod{p}$. Then $x^p + y^p = z^p$, which rearranged is $x^p + (-z)^p = (-y)^p$, so if we rename $-z = Y$ and $-y = Z$, then $x \not\equiv Y \pmod{p}$.

So we may indeed assume $x \not\equiv y \pmod{p}$. We also assume x, y, and z are pairwise coprime, which we have discussed before.

We go about factorising $x^p + y^p = z^p$ over $K = \mathbb{Q}(\xi_p)$, getting

$$\prod_{i=0}^{p-1}(x + \xi^i y) = z^p,$$

where we've called $\xi = \xi_p$. Then as ideals

$$\prod_{i=0}^{p-1}(x + \xi^i y)\mathcal{O}_K = (z\mathcal{O}_K)^p.$$

We'll prove the theorem in five steps.

Step 1: The ideals $(x + \xi^i y)\mathcal{O}_K$ are pairwise coprime.

To see this, note that the gcd of $(x+\xi^j y)\mathcal{O}_K$ and $(x+\xi^i y)\mathcal{O}_K$ must contain

$$(x + xi^j y) - (x + \xi^i y) = \xi^j y(1 - \xi^{i-j}),$$

supposing $i > j$. Hence a common prime factor must necessarily divide $\xi^j y(1 - \xi^{i-j})$, which means it must divide (y) or $(1 - \xi^{i-j})$, since ξ^j is a unit. For the latter we have $(1 - \xi^{i-j}) = (1 - \xi)$ since

$$\frac{1 - \xi^{i-j}}{1 - \xi} \in \mathcal{O}_K^\times.$$

Now if it divides (y), then it must also divide (z) in $\mathcal{O}_K$, but this is a contradiciton since $\gcd(y, z) = 1$.

On the other hand, if it divides $(1 - \xi)$, which is a prime ideal, then it must be equal to $(1-\xi)$ by maximality of nonzero prime ideals in Dedekind domains. Hence it implies $(1 - \xi) \mid z\mathcal{O}_K$, taking norms yields $\mathrm{N}(1 - \xi) \mid \mathrm{N}(z)$, or in other words $\pm p \mid z^p$, implying $p \mid z$, which is a contradiction since $p \nmid xyz$. □

Lecture 16 Kummer's Theorem, continued

16.1 Proof continued

Proof of Kummer's theorem, continued. Step 2: We show that

$$(x^i_\xi y) = I_i^p$$

where I_i is a principal ideal.

We know from Step 1 that $(x + \xi^i y) = I_i^p$ for some ideal $I_i \subset \mathcal{O}_K$, by prime factorisation of ideals.

Now since $p \nmid h(K)$, then there exist $a, b \in \mathbb{Z}$ such that $ap + bh(K) = 1$. In $\mathrm{Cl}(K)$, we have

$$[I_i] = [I_i]^{ap+bh(K)} = [I_i]^a p = [I_i^p]^a = [(x + \xi^i y)]^a = 1$$

since $h(K)$ is the order of the class group, and since $(x+\xi^i y)$ is clearly principal. Hence I_i is principal, because it is in the same ideal class as a principal ideal.

Therefore $(x + \xi^i y) = (\alpha_i)^p = (\alpha_i^p)$ for some $\alpha_i \in \mathcal{O}_K$. For $i = 1$, we have $x + \xi y = \varepsilon\alpha^p$, with $\alpha = \alpha_1$ and $\varepsilon \in \mathcal{O}_K^\times$.

Date: March 1st, 2018.

By the lemma, $\varepsilon = u \cdot \xi^r$ with $u \in \mathbb{R}$ and $r \in \mathbb{Z}$, and $\alpha^p \equiv a^p \equiv d \pmod{(1-\xi)^p}$. Hence $x + \xi y \equiv u\xi^r d \pmod{(1-\xi)^p}$.

Step 3: Let us show that $r \not\equiv 0, 1 \pmod p$, and if $p > 3$, then $2r \not\equiv 1 \pmod p$.

To show this, note that $(1-\xi^{-1})^p = (1-\xi)^p$ as ideals in $\mathcal{O}_K$ since

$$\frac{1-\xi^{-1}}{1-\xi} \in \mathcal{O}_K^\times,$$

so they differ by a unit.

Next $\xi^{-r}(x+\xi y) \equiv ud \pmod{(1-\xi)^p}$, and taking complex conjugates we have

$$\xi^{-r}(x+\xi y) \equiv \xi^r(x+\xi^{-1}y) \pmod{(1-\xi)^p},$$

where again we should strictly speaking conjugate the ideal, but by the above they're the same.

Expanding we thus have

$$\xi^{-r}x + \xi^{1-r}y \equiv \xi^r x + \xi^{r-1}y \pmod{(1-\xi)^p}.$$

Therefore if $r \equiv 0 \pmod p$, then $\xi^r \equiv 1$, in which case $\xi y \equiv \xi^{-1}y \pmod{(1-\xi)^p}$, so $y(\xi - \xi^{-1}) \equiv 0 \pmod{(10\xi)^p}$, but

$$\xi - \xi^{-1} = -\xi^{-1}(1-\xi^2) = \underbrace{-\xi^{-1}\frac{1-\xi^2}{1-xi}}_{\in \mathcal{O}_K^\times}(1-\xi)$$

so $(\xi - \xi^{-1}) = (1-\xi)$ as ideals, so $y \equiv 0 \pmod{(1-\xi)^{p-1}}$, whence $(1-\xi)^{p-1} = p\mathcal{O}_K \mid (y)$. Taking norms $p^{p-1} \mid y^{p-1}$, so $p \mid y$, a contradiction. Hence $r \not\equiv 0 \pmod p$.

If $r \equiv 1 \pmod p$, then $\xi^r \equiv r$, and we get $x(\xi^{-1} - \xi) \equiv 0 \pmod{(1-\xi)^p}$, so by identical argument $p \mid x$, a contradiction.

Finally let $p > 3$. Then if $2r \equiv 1 \pmod p$, $\xi^{2r} \equiv \xi$, whence $\xi^{2r-1} = 1$.

Multiplying the equation we've been working with by ξ^r, then, yields

$$x + \xi y = \xi^{2r}x + \xi^{2r-1}y \equiv \xi x + y \pmod{(1-\xi)^p}.$$

Hence

$$(x-y) + (y-x)\xi = (x-y)(1-\xi) \equiv 0 \pmod{(10\xi)^p}.$$

Since $(1-\xi)^p = (1-\xi)p\mathcal{O}_K$, this if the same as

$$x - y \equiv 0 \pmod p,$$

so $x \equiv y \pmod p$, a contradiction.

Step 4: The theorem is true for $p > 3$.

By Step 3, for $p > 3$, all of ξ^{-r}, ξ^{1-r}, ξ^r, and ξ^{r-1} are all distinct. Hence they are linearly independent over $\mathbb{Z}$.

Therefore

$$x\xi^{-r} + y\xi^{1-r} - x\xi^r - y\xi^{r-1} \equiv 0 \pmod{(1-\xi)^p},$$

factoring $(1-\xi)$ we have $x \equiv 0 \pmod p$, a contradiction.

Step 5: The theorem is true for all odd p.

It only remains to consider $p = 3$. We must have $x^3 \equiv \pm 1 \pmod 9$ (just consider $x = 0, 1, 2$), but $x = 0$ is not an option since $xyz \neq 0$.

Hence $x^3 + y^3 \equiv (\pm 1) + (\pm 1) \pmod 9$, so it's ± 2 or 0, but z^3 can't be either of those by the same reasoning. $\square$

Lecture 17 Local Fields

17.1 Valuations

Definition 17.1.1 (Valuation)**.** Let K be a field. A ***valuation*** on K is a function $|\cdot|\colon K \to \mathbb{R}_{\geq 0}$ such that

(*i*) $|x| \geq 0$ and $|x| = 0$ if and only if $x = 0$,

(*ii*) $|xy| = |x||y|$, and

(*iii*) $|x + y| \leq |x| + |y|$, i.e. the triangle inequality.

Clearly $|1| = |-1| = 1$ (take $x = y = \pm 1$ in (*ii*)). Similarly $|-x| = |x|$.

Example 17.1.2. We always have the trivial valuation, namely $|x| = 1$ for all $x \in K^\times$, and $|0| = 0$.

In $\mathbb{R}$ and $\mathbb{C}$, the usual absolute value is a valuation. We will usually denote it $|\cdot|_\infty$ in order to avoid ambiguity.

Let K be a number field and let $\sigma\colon K \hookrightarrow \mathbb{C}$ be an embedding. Then $|x|_\sigma = |\sigma(x)|_\infty$ is a valuation. (That this is the case follows from σ being a homomorphism, then using the fact that $|\cdot|_\infty$ is a valuation on $\mathbb{R}$.)

Let K be a number field and let $P \subset \mathcal{O}_K$ be a nonzero prime ideal. For $x \in K^\times$, define $(x) = P^a q_1 q_2 \cdots$, with $a \in \mathbb{Z}$, i.e. prime factor the ideal (x) and count the number of times P occurs (hence $a = 0$ if P isn't a divisor of (x)). Define $\operatorname{ord}_P(x) = a$. Then

$$|x|_P = \mathrm{N}_K(P)^{-\operatorname{ord}_P(x)}$$

is a valuation.

In particular, if $K = \mathbb{Q}$, write $x = p^a \cdot m/n$ with $p \nmid mn$, $a \in \mathbb{Z}$, then $|x|_p = p^{-a}$ is a valuation, namely the so-called ***p-adic valuation***. ▲

Definition 17.1.3. Two valuations $|\cdot|_1$ and $|\cdot|_2$ on K are ***equivalent*** if there exists some $c > 0$ such that $|x|_1 = |x|_2^c$ for all $x \in K$.

Remark 17.1.4. Let $|\cdot|$ be a valuation on K. We can then define the distance between two points $x, y \in K$ as $d(x, y) = |x - y|/$

Then K is a metric space and hence a topological space. This makes K into a ***topological field***, meaning that $K \times K \to K$ by $(x, y) \mapsto x + y$ and $(x, y) \mapsto xy$ are continuous maps, and so are $x \mapsto -x$ and $x \mapsto x^{-1}$ (the last one of course on $K^\times$).

In view of this, equivalent valuations induce the same topology.

It turns out that on $\mathbb{Q}$, the only nontrivial valuations are $|\cdot|_\infty$ and $|\cdot|_p$, for p prime. We will work toward proving this.

Proposition 17.1.5. *Let $|\cdot|_1$ and $|\cdot|_2$ be two valuations on K with $|\cdot|_1$ nontrivial. Suppose $|x|_1 < 1$ implies $|x|_2 < 1$. Then $|\cdot|_1$ and $|\cdot|_2$ are equivalent.*

Proof. First, we claim that if $|x|_2 < 1$, then $|x|_1 < 1$ as well, whereby $|x|_1$ if and only if $|x|_2$.

Date: March 6th, 2018.

Since $|\cdot|_2$ is nontrivial, there exists some $y \in K^\times$ such that $|y|_1 \neq 1$. We may assume $0 < |y|_1 < 1$, since otherwise we can just work with y^{-1}. Then by assumption $|y|_2 < 1$.

Now suppose there exists some x such that $|x|_2 < 1$ but $|x|_1 \geq 1$. Then

$$\left|\frac{y}{x^n}\right|_1 = \frac{|y|_1}{|x|_1^n} \leq |y|_1 < 1$$

for some sufficiently big n. Now since $|y/x^n|_1 < 1$, we must by assumption have $|y/x^n|_2 < 1$, meaning that $|y|_2 < |x|_2^n$, which goes to 0 as $n \to \infty$.

Hence $|y|_2 < 0$, implying $y = 0$, which is a contradiction since $0 < |y|_1 < 1$.

Now let $z = 1/y$. Then $|z|_1 > 1$ and $|z|_2 > 1$. For each $x \in K^\times$, $|x|_1 = |z|_1^{B_1}$ and $|x|_2 = |z|_2^{B_2}$ for some $B_1, B_2 \in \mathbb{R}$, dependent on x.

We claim that $B_1 = B_2$. To see this, consider any $n/m \in \mathbb{Q}$ with $n/m < B_1$. This is equivalent with $|x|_1 = |z|_1^{B_1} > |z|_1^{n/m}$ since $|z|_1 > 1$. This in turn is equivalent with $|x^m|_1 > |z|_1^n$, if and only if $|x^{-m}z^n|_1 < 1$.

Bt the claim this is equivalent with $|x^{-m}z^n|_2 < 1$, if and only if $|x|_2 > |z|_2^{n/m}$, if and only if $|z|_2^{B_2} > |z|_2^{n/m}$, if and only if $B_2 > n/m$, since $|z|_2 > 1$.

Hence $B_1 = B_2 = B$.

So $|x|_1 = |z|_1^B$ and $|x|_2 = |z|_2^B$ with B depending on x. Now write $|z|_1 = |z|_2^c$ for some $c > 0$. Then

$$|x|_1 = |z|_1^B = (|z|_2^c)^B = (|z|_2^B)^c = |x|_2^c.$$

Notice how c is independent of x, so $|\cdot|_1$ and $|\cdot|_2$ are equivalent. □

Corollary 17.1.6. *Two valuations $|\cdot|_1$ and $|\cdot|_1$ are equivalent if and only if they define the same topology.*

Proof. The forward direction is trivial since if the valuations are equivalent $|x|_1 = |x|_2^c$ for some c, so open sets in one will be open sets in the other.

The reverse direction requires a little bit more work. Suppose $|\cdot|_1$ and $|\cdot|_2$ induce the same topology. Then

$$\lim_{n\to\infty} x^n = 0$$

with respect to $|\cdot|_1$ if and only if it does the same with respect to $|\cdot|_2$. Hence $|x|_1^n \to 0$ in $\mathbb{R}$, and $|x|_2^n \to 0$ in $\mathbb{R}$, whence $|x|_1 < 1$ if and only if $|x|_2 < 1$, so the valuations are equivalent. □

Definition 17.1.7 (Non-archimedean valuation)**.** A valuation $|\cdot|$ is called ***non-archimedean*** if

$$|x + y| \leq \max\{\, |x|, |y| \,\},$$

called the ***strong triangle inequality***.

Otherwise the valuation is called ***archimedean***.

Definition 17.1.8 (Discrete valuation)**.** A valuation is ***discrete*** if there exists $\delta > 0$ such that $1 - \delta < |x| < 1 + \delta$ implies $|x| = 1$.

Suppose that $|y| = a \in \mathbb{R}$. If $a - \delta' < |x| < a + \delta'$, then

$$1 - \frac{\delta'}{a} < \frac{|x|}{|y|} < 1 + \frac{\delta'}{a}.$$

Hence if we choose δ' small enough, so that $\delta'/a < \delta$, then this implies $|x/y| = 1$, i.e. $|x| = |y|$, so $|\cdot|$ takes discrete values not only around 1, but everywhere.

There is a reasonably straight forward condition for a valuation being non-archimedean:

Proposition 17.1.9. *The valuation $|\cdot|$ is non-archimedean if and only if $|n| \leq A$ for some $A > 0$ for all $n \in \mathbb{N}$.*

Proof. The forward direction is simple. Consider

$$|2| = |1 + 1| \leq \max\{\, |1|, |1| \,\} = 1.$$

By induction we can do the same thing and get $|n| \leq 1$ for all $n \in \mathbb{N}$.

For the opposite direction, take $x, y \in K$ with $|x| \geq |y|$. Then we have

$$|x|^m |y|^{n-m} \leq |x|^m |x|^{n-m} = |x|^n$$

for all $0 \leq m \leq n$. Then

$$|x + y|^n = |(x + y)^n| = \Big| \sum_{m=0}^{n} \binom{n}{m} x^m y^{n-m} \Big| \leq \sum_{m=0}^{n} \Big| \binom{n}{m} \Big| |x|^m |y|^{n-m}.$$

Now the binomial coefficient is an integer, so its valuation is by assumption bounded by A, and the two last factors are bounded by $|x|^n$ by the above, so

$$|x + y|^n \leq A(n + 1)|x|^n.$$

Taking nth roots,

$$|x + y| \leq A^{1/n}(n + 1)^{1/n}|x| \to |x|$$

as $n \to \infty$. Hence

$$|x + y| \leq |x| = \max\{\, |x|, |y| \,\},$$

so the valuation is non-archimedean. □

Remark 17.1.10. The strong triangle inequality implies that if $|x| \neq |y|$, then $|x + y| = \max\{\, |x|, |y| \,\}$.

To see this, suppose $|x| > |y|$. Then

$$|x| = |(x + y) + (-y)| \leq \max |x + y|, |y|,$$

but $|x| > |y|$, so $|x| \leq |x + y|$. The other inequality is true by the strong triangle inequality itself.

Lecture 18 Ostrowski's Theorem

18.1 Ostrowski's Theorem

Theorem 18.1.1 (Ostrowski)**.** *Every nontrivial valuation on $\mathbb{Q}$ is equivalent to one of $|\cdot|_\infty$, the usual absolute value, or $|\cdot|_p$, with p prime.*

Remark 18.1.2. Note that $|\cdot|_\infty$, $|\cdot|_p$ are pairwise inequivalent. To see this, find some x that violates $|x|_1 < 1$ if and only if $|x|_2 < 1$.

Proof. First, let $|\cdot|$ be a nontrivial non-archimedean valuation on $\mathbb{Q}$. Then for $n \in \mathbb{N}$, we have $|n| \leq 1$, and there exists a prime p such that $|p| < 1$ (since otherwise $|p| = 1$ for all p, making the valuation trivial, since it means that $|n| = 1$ for all $n \in \mathbb{Z}$, so $|x| = 1$ for all $x \in \mathbb{Q} \setminus \{0\}$).

Now consider $I = \{ n \in \mathbb{Z} \mid |n| < 1 \}$. This is an ideal of $\mathbb{Z}$, clearly, since $|k| \leq 1$ for all $k \in \mathbb{Z}$, so $kn \in I$ if $n \in I$, and by the strong triangle inequality $n_1 + n_2 \in I$ if $n_1, n_2 \in I$.

Moreover $p\mathbb{Z} \subset I \subsetneq \mathbb{Z}$ since $|1| = 1$, but $p\mathbb{Z}$ is prime, hence maximal (we're in a Dedekind domain and it's nonzero), so $p\mathbb{Z} = I$.

Now for any $n \in \mathbb{Z}$, wriet $n = mp^a$ with $p \nmid m$. Then $|m| = 1$ since $m \notin p\mathbb{Z} = I$, but $|m| \leq 1$. Hence $|n| = |p|^a$, and also $|n|_p^c = |p|^a$ for some c, since $|n|_p = p^{-a}$.

So

$$c = -\frac{\log|p|}{\log p},$$

implying $|x| = |x|_p^c$ for every $x \in \mathbb{Q}$, so $|\cdot|$ is equivalent to $|\cdot|_p$ on $\mathbb{Q}$.

Next, let $|\cdot|$ be a nontrivial archimedean valuation on $\mathbb{Q}$. We claim that for all integers $n, m > 1$,

$$|m|^{1/\log m} = |n|^{1/\log n}.$$

To see this, write $m = a_0 + a_1 n + a_2 n^2 + \ldots + a_r n^r$, with $0 \leq a_i \leq n-1$ and $a_r \neq 0$, i.e. expand m in base n.

Hence $n^r \leq m < n^{r+1}$ inplies

$$r \leq \frac{\log m}{\log n} < r + 1,$$

and $|a_i| = |1 + 1 + \ldots + 1| \leq a_i|1| = a_i < n$. By the triangle inequality,

$$|m| \leq \sum_{i=0}^{r} |a_i||n|^i \leq (r+1)nN^r \leq \Big(\frac{\log m}{\log n} + 1\Big) nN^{\log m/\log n}.$$

where $N = \max\{1, |n|\}$.

Replace m by m^t, take $t \in \mathbb{N}$, and then take tth roots, we get

$$|m| \leq \Big(\frac{t\log m}{\log n} + 1\Big)^{1/t} n^{1/t} N^{\log m/\log n}$$

for every $t \in \mathbb{N}$. The first two terms, the ones depending on t, go to 1 as $t \to \infty$, whence

$$|m| \leq N^{\log m/\log n}.$$

Date: March 8th, 2018.

There are now two cases to consider. First, $|n| > 1$ for all $n > 1$, in which case $N = |n|$. Then

$$|m| \leq |n|^{\log m / \log n}$$

whereby

$$|m|^{1/\log m} \leq |n|^{1/\log n},$$

where if we switch the roles of m and n and repeat we get equality.

Secondly, suppose there exists some $n > 1$ such that $|n| \leq 1$. Fixing this n, we have $N = 1$, and if we consider all integers $m > 1$ we get $|m| \leq 1$, whence $|\cdot|$ is bounded on integers, which by our earlier proposition means that $|\cdot|$ is non-archimedean, a contradiction.

Now let $S = |n|^{1/\log n}$ for some $n > 1$, which by our claim is independent of n. Then $|n| = S^{\log n}$, whence we set $S = e^c$, for $c = \log S$.

Then

$$|n| = e^{c \log n} = n^c = |n|_\infty^c,$$

so $|x| = |x|_\infty^c$ for all $x \in \mathbb{Q}$. □

18.2 Completions

In the discussion that follows we'll have $|\cdot|$ be a valuation on K.

Definition 18.2.1 (Cauchy sequence)**.** A sequence $\{ a_n \}$ is ***Cauchy*** if for every $\varepsilon > 0$ there exists some $N \in \mathbb{N}$ such that $|a_n - a_m| < \varepsilon$ for every $n, m \geq N$.

Example 18.2.2. If

$$\lim_{n \to \infty} a_n = a$$

in K, i.e. $|a_n - a| \to 0$ as $n \to \infty$, then $\{ a_n \}$ is Cauchy. ▲

Definition 18.2.3 (Complete space)**.** If every Cauchy sequence converges in K, then we say that K is ***complete*** with respect to $|\cdot|$.

Definition 18.2.4 (Completion)**.** A field $\widehat{K} \supset K$ with valuation $|\cdot|'$ extending $|\cdot|$ on K is the ***completion*** of K with respect to $|\cdot|$ if

(*i*) $\widehat{K}$ is complete with respect to $|\cdot|'$, and

(*ii*) K is dense in $\widehat{K}$.

The completion exists and is unique. We'll prove this in two parts.

Proof of existence. Let R be the set of all Cauchy sequences in K. Then R is a ring, since termwise operations $\{ a_n \} + \{ b_n \} = \{ a_n + b_n \}$ and $\{ a_n \}\{ b_n \} = \{ a_n b_n \}$ maintain Cauchy by the triangle inequality.

Moreover let M be the set of all null sequences in K, by which we mean sequences $\{ a_n \}$ such that

$$\lim_{n \to \infty} a_n = 0.$$

Then M is a maximal ideal in R, and so we define $\widehat{K} = R/M$, which is a field since M is maximal.

For $a = \{ a_n \} + M$, define

$$|a|' = \lim_{n \to \infty} |a_n|$$

on $\widehat{K}$. This limit exists since

$$\big||a_n| - |a_m|\big|_\infty \leq |a_n - a_m| \to 0$$

as $n, m \to \infty$, where the inequality is just the triangle inequality on $\mathbb{R}$, and the convergence is by $\{ a_n \}$ being Cauchy in K.

We can embed K into $\widehat{K}$ by $a \mapsto \{ a_n \} + M$, where $\{ a_n \}$ is the constant sequence $a_n = a$.

Then $|\cdot|'$ is a valuation on $\widehat{K}$, $\widehat{K}$ is complete with respect to $|\cdot|'$, and K is dense in $\widehat{K}$. For the last one, given $a = \{ a_n \} + M \in \widehat{K}$, take $\{ a_n \}$ in K and consider embedding each term in the sequence as above. Then this sequence converves to a in $\widehat{K}$. □

Proof of uniqueness. Let $(\widehat{K}, |\cdot|)$ and $(\widehat{K}', |\cdot|')$ be two completions of K. Define $\sigma \colon \widehat{K} \to \widehat{K}'$ in the following way. Given $x \in \widehat{K}$, K is dense in $\widehat{K}$, so find $\{ x_n \}$ in K such that $x_n \to x$ in $\widehat{K}$.

Look at $\{ x_n \}$ in $K \subset \widehat{K}'$. Then $x_n \to y$ for some $y \in \widehat{K}'$, since the sequence is Cauchy and K is dense in $\widehat{K}'$. Hence define $\sigma(x) = y$.

Then σ is well-defined, i.e. it does not depend on the choice of sequence $\{ x_n \}$, and moreover σ is a K-isomorphism, and $|x| = |\sigma(x)|'$. □

Theorem 18.2.5 (Ostrowski)**.** *Let K be a number field and let $|\cdot|$ be some archimedean valuation on K. Let $\widehat{K}$ be a completion of K with respect to $|\cdot|$. Then there exists an isomorphism σ from $\widehat{K}$ to $\mathbb{R}$ or $\mathbb{C}$ satisfying $|x| = |\sigma(x)|_\infty^s$ for all $x \in \widehat{K}$ for some fixed $s \in \mathbb{R}$, $S > 0$.*

Lecture 19 Ostrowski's Theorem continued

19.1 Proof of Ostrowki's Theorem

Before we prove Ostrowski's theorem we will prove the following:

Theorem 19.1.1 (Approximation theorem)**.** *Let $|\cdot|_1, |\cdot|_2, \ldots, |\cdot|_n$ be pairwise inequivalent nontrivial valuations on K. Let K_i be the completion of K with respect to $|\cdot|_i$. Consider $K_1 \times K_2 \times \ldots \times K_n$ with the product topology, i.e. the basis for the open sets are the open sets in the respective K_i.*

Define $d \colon K \to K_1 \times K_2 \times \ldots \times K_n$, the **diagonal map** *defined by $x \mapsto (x, x, \ldots, x)$.*

Then $d(K)$ is dense in $K_1 \times K_2 \times \ldots \times K_n$.

To prove this we require the following lemma.

Lemma 19.1.2. *There exists a $z \in K$ such that $|z|_1 > 1$ and $|z|_i < 1$ for all $i = 2, 3, \ldots, n$.*

Proof. We prove it by induction on n. For $n = 1$, since $|\cdot|_1$ and $|\cdot|_2$ are inequivalent, there exists some $x \in K$ such that $|x|_1 < 1$ and $|x|_2 \geq 1$, and similarly there is some $y \in K$ such that $|y|_2 < 1$ and $|y|_1 \geq 1$.

Date: March 20th, 2018.

Hence if we take $z = y/x$ we get

$$|z|_1 = \frac{|y|_1}{|x|_1} > 1$$

and

$$|z|_2 = \frac{|y|_2}{|x|_2} < 1.$$

For $n > 2$, suppose there exists $x \in K$ such that $|x|_1 > 1$ and $|x|_i < 1$ for all $i = 2, 3, \ldots, n-1$.

By the $n = 2$ case, pairing $|\cdot|_1$ and $|\cdot|_n$, there exists some $y \in K$ such that $|y|_1 > 1$ and $|y|_n < 1$.

Now we have two options. If $|x|_n \leq 1$, then take $z = x^N y$, whence $|z|_1 = |x|_1^N |y|_1 > 1$ and $|z|_i = |x|_i^N |y|_i < 1$ for $i = 2, 3, \ldots, n-1$, taking N to be sufficiently large. Moreover $|z|_n = |x|_n^N |y|_n < 1$.

If, on the other hand, $|x|_n > 1$, we take $z = x^N y/(1 + x^N)$. Then if we consider the limit of

$$\frac{x^N y}{1 + x^N}$$

as $N \to \infty$, we get the following: with respect to $|\cdot|_1$, it approaches y, and $|y|_1 > 1$.

With respect to $|\cdot|_i$, for $i = 2, 3, \ldots, n-1$, it goes to 0, since $|x|_i < 1$.

Finally with respect to $|\cdot|_n$ it goes to y, and $|y|_n < 1$. □

Proof of Ostrowski's theorem. By the lemma there exists $z_i \in K$ such that $|z_i|_i > 1$ and $|z_i|_j < 1$ for $i \neq j$, for $i = 1, 2, \ldots, n$. Notice how $z_i^N/(1 + z_i^N)$ approaches 1 with respect to $|\cdot|_i$, but 0 with respect to $|\cdot|_j$, for $j \neq i$, as $N \to \infty$.

Given $x_1, x_2, \ldots, x_n \in K$, consider

$$y_N = \sum_{i=1}^{N} x_i \frac{z_i^N}{1 + z_i^N}.$$

Then $y_N \to x_i$ with respect to $|\cdot|_i$.

Hence given $(x_1, x_2, \ldots, x_n) \in K \times K \times \ldots \times K \subset K_1 \times K_2 \times \ldots \times K_n$, we have $d(y_N) \to (x_1, x_2, \ldots, x_n)$. But $K \times K \times \ldots \times K$ is dense in $K_1 \times K_2 \times \ldots \times K_n$ by definition of completion, whereby $d(K)$ is dense in $K_1 \times K_2 \times \ldots \times K_n$. □

The part of this result we really need is the following immediate corollary:

Corollary 19.1.3. *Let $|\cdot|_i$, $i = 1, 2, \ldots, n$ be pairwise inequivalent valuations on K. Given $\varepsilon > 0$ and $a_1, a_2, \ldots, a_n \in K$, there exists $x \in K$ such that $|x - a_i|_i < \varepsilon$ for all $i = 1, 2, \ldots, n$.*

Theorem 19.1.4 (Ostrowski)**.** *Let $\widehat{K}$ be a field extension of $\mathbb{Q}$ that is complete with respect to an archimedian valuation $|\cdot|$. Then there exists an isomorphism σ from $\widehat{K}$ to $\mathbb{R}$ or $\mathbb{C}$ satisfying $|x| = |\sigma(x)|_\infty^s$ for every $x \in \widehat{K}$ for some fixed $s > 0$.*

Note that strictly speaking Ostrowski proved a slightly more general result, without the field being an extension of $\mathbb{Q}$, and just required that it was of characteristic 0.

Proof. We prove it in three parts.

Step 1: Reduce to the case $|\cdot| = |\cdot|_\infty$ on $\mathbb{Q}$.

To see that this suffices, suppose $|\cdot|$ is an archimedean valuation on $\mathbb{Q}$. Hence $|\cdot| = |\cdot|_\infty^c$ on $\mathbb{Q}$ for some c. Now consider $|\cdot|_1 = |\cdot|^{1/c}$ on $\widehat{K}$. This is an archimedean valuation, and $|\cdot|_1 = |\cdot|_\infty$ on $\mathbb{Q}$.

Thus if the theorem is true for $|\cdot|_1$, i.e. $|x| = |\sigma(x)|_\infty^s$ for all $x \in \widehat{K}$, then $|x| = |x|_1^c = |\sigma(x)|_\infty^{cs}$ for all $x \in \widehat{K}$.

Now let $\widehat{\mathbb{Q}}$ be the completion of $\mathbb{Q}$ in $\widehat{K}$ with respect to $|\cdot| = |\cdot|_\infty$ on $\mathbb{Q}$. By the uniqueness of completion, and since completing $\mathbb{Q}$ with respect to $|\cdot|_\infty$, we must have $\widehat{\mathbb{Q}} \cong \mathbb{R}$, so there exists some $\mathbb{Q}$-isomorphism $\sigma\colon \widehat{\mathbb{Q}} \to \mathbb{R}$ such that $|x| = |\sigma(x)|_\infty$ for every $x \in \widehat{\mathbb{Q}}$.

Without loss of generality we can therefore assume $\mathbb{R} \subset \widehat{K}$, and $|\cdot| = |\cdot|_\infty$ on $\mathbb{R}$.

Step 2: It suffices to show for each $a \in \widehat{K}$ it satisfies a quadratic equation over $\mathbb{R}$. This would mean that $\mathbb{R} \subset \widehat{K} \subset \mathbb{C} = \mathbb{R}[\sqrt{-1}]$. But since $[\mathbb{C} : \mathbb{R}] = 2$, there can be no intermediate fields, so $\widehat{K} = \mathbb{R}$ or $\widehat{K} = \mathbb{C}$.

Consider the continuous map $f\colon \mathbb{C} \to \mathbb{R}_{\geq 0}$ defined by

$$f(z) = \left|a^2 - (z + \overline{z})a + z\overline{z}\right|,$$

which is then the valuation on $\widehat{K}$. Notice how $z + \overline{z} = 2\operatorname{Re}(z)$ and $z\overline{z} = |z|^2$, so they are real.

Now since this is a quadratic expression in z, we must have

$$\lim_{z\to\infty} f(z) = \infty.$$

Hence $f(z)$ has a minimum, say m. Thus

$$S = \{\, z \in \mathbb{C} \mid f(z) = m \,\} \neq \varnothing,$$

and S is bounded and closed in $\mathbb{C}$, whence it is compact. Hence there exists some $z_0 \in S$ such that $|z_0|_\infty \geq |z|_\infty$ for every $z \in S$ (since continuous functions map compact sets to compact sets).

We claim that $m = 0$. If this is the case we're done, since it implies

$$a^2 - (z_0 + \overline{z_0})a + z_0\overline{z_0} = 0,$$

a quadratic over $\mathbb{R}$, so a solves a quadratic polynomial over $\mathbb{R}$ and hence $\mathbb{R} \subset \widehat{K} \subset \mathbb{C}$.

Suppose $m > 0$ and consider

$$g(x) = x^2 - (z_0 + \overline{z_0})x + z_0\overline{z_0} + \varepsilon \in \mathbb{R}[x]$$

for $0 < \varepsilon < m$. Then $g(x)$ has two roots, $z_1, \overline{z_1} \in \mathbb{C}$ with $z_1\overline{z_1} = z_0\overline{z_0} + \varepsilon$, meaning that $|z_1|_\infty^2 = |z_0|_\infty^2 + \varepsilon$. This implies $|z_1|_\infty > |z_0|_\infty$, whence $z_1 \notin S$, wherefore $f(z_1) > m$.

On the other hand, fix $n \in \mathbb{N}$ and consider

$$G(x) = (g(x) - \varepsilon)^n - (-\varepsilon)^n = \prod_{i=1}^{2n}(x - \alpha_i) = \prod_{i=1}^{2n}(x - \overline{\alpha_i}) \in \mathbb{R}[x],$$

where $\alpha_1, \alpha_2, \ldots, \alpha_n \in \mathbb{C}$ are the roots of $G(x)$.

Now

$$G(z_1) = (g(z_1) - \varepsilon)^n - (-\varepsilon)^n = 0$$

so z_1 is a root of $G(x)$, say $z_1 = \alpha_1$.

Next,

$$G(x)^2 = \prod_{i=1}^{2n}(x - \alpha_i)(x - \overline{\alpha_i}) = \prod_{i=1}^{2n}(x^2 - (\alpha_i + \overline{\alpha_i})x + \alpha_i\overline{\alpha_i}),$$

which means that

$$|G(a)|^2 = \prod_{i=1}^{2n} f(\alpha_i) \geq f(\alpha_1)m^{2n-1} = f(z_1)m^{2n-1}.$$

From the definition of $G(x)$ we also have

$$|G(a)| \leq |a^2 - (z_0 + \overline{z_0})a + z_0\overline{z_0}|^n + |-\varepsilon|^n = f(z_0)^n + \varepsilon^n = m^n + \varepsilon^n.$$

Therefore $f(z_1)m^{2n-1} \leq (m^n + \varepsilon^n)^2$ so

$$\frac{f(z_1)}{m} \leq \left(1 + \left(\frac{\varepsilon}{m}\right)^n\right)^2 \to 1$$

as $n \to \infty$, meaning that $f(z_1) \leq m$, which contradicts $f(z_1) > m$. Hence $m = 0$, as claimed.

Step 3: let us show that $|\cdot| = |\cdot|_\infty$ on $\widehat{K}$.

If $\widehat{K} = \mathbb{R}$, we are done. If $\widehat{K} = \mathbb{C}$, then we claim that $|\cdot|$ and $|\cdot|_\infty$ are equivalent on $\widehat{K} = \mathbb{C}$.

Then we would have $|\cdot| = |\cdot|_\infty^c$ on $\widehat{K}$, but $|\cdot| = |\cdot|_\infty$ on $\mathbb{R}$, so $c = 1$.

Now for any $z = a + bi \in \mathbb{C}$, with $a, b \in \mathbb{R}$, we have

$$|z| = |a + bi| \leq |a| + |i||b| = |a|_\infty + |b|_\infty \leq |z|_\infty + |z|_\infty$$

whereby $|z| \leq 2|z|_\infty$.

Suppose now that $|\cdot|$ and $|\cdot|_\infty$ are inequivalent on $\mathbb{C}$. By the approximation theorem, for any $\varepsilon > 0$ there exists some $\alpha \in \mathbb{C}$ such that $|\alpha - 1| < \varepsilon$ and $|\alpha|_\infty < \varepsilon$. In other words, use the approximation theorem on $\mathbb{C} \times \mathbb{C}$ and find α such that $(1, 0)$ is close to (α, α).

Hence

$$\big||\alpha| - |1|\big|_\infty \leq |\alpha - 1| < \varepsilon$$

whereby $1 - \varepsilon < |\alpha| < 1 + \varepsilon$.

By $|z| \leq 2|z|_\infty$ above, then $|\alpha| \leq 2|\alpha|_\infty < \varepsilon$, but this is a contradiction since with ε small we can't have $|\alpha|$ close to 1 and 0 simultaneously. □

Example 19.1.5. Let K be a number field and $\sigma\colon K \hookrightarrow \mathbb{C}$ an embedding. Define a valuation on K by $|x| = |\sigma(x)|_\infty$ for $x \in K$. This is archimedean, so the completion of K with respect to $|\cdot|$ is $\widehat{K}$, which is isomorphic to $\mathbb{R}$ if $\sigma(K) \subset \mathbb{R}$, and isomoprhic to $\mathbb{C}$ if $\sigma(K) \not\subset \mathbb{R}$. ▲

Lecture 20 Local Fields

20.1 Local Fields

In what follows K is any field and $|\cdot|$ is a nontrivial valuation on K.

Definition 20.1.1 (Valuation Ring)**.** The set $\mathcal{O}_K = \{\, x \in K \,|\, |x| \leq 1 \,\}$ is called the ***valuation ring*** of K and $\mathcal{M}_K = \{\, x \in K \mid |x| < 1 \,\}$ is the maximal ideal of $\mathcal{O}_K$.

Lemma 20.1.2. *(i) $\mathcal{O}_K$ is an integrally closed integral domain, $\mathcal{O}_K^\times = \{\, x \in K \mid |x| = 1 \,\}$, and K is the field of fractions of $\mathcal{O}_K$.*

(ii) $\mathcal{M}_K$ is the unique maximal ideal of $\mathcal{O}_K$, i.e. $\mathcal{O}_K$ is a local ring.

(iii) If $|\cdot|$ is discrete, then $\mathcal{O}_K$ is a principal ideal domain. In fact, $\mathcal{O}_K$ is a discrete valuation ring, and it is also a Dedekind domain.

Proof. (i) Let us first show that $\mathcal{O}_K$ is a ring. Let $x, y \in \mathcal{O}_K$. Then $|x| = |-x| \leq 1$, whereby $-x \in \mathcal{O}_K$. Similarly $|xy| = |x||y| \leq 1 \cdot 1 \leq 1$, so $xy \in \mathcal{O}_K$, and finally $|x + y| \leq \max\{\, |x|, |y| \,\} \leq 1$, so $x + y \in \mathcal{O}_K$.

Now since this is a subring of a field, it can't contain any zero divisors, and so is an integral domain.

To see that it is integrally closed, suppose $x \in K$ is integral over $\mathcal{O}_K$. Then

$$x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 = 0$$

with $a_i \in \mathcal{O}_K$. Taking valuations and rearranging,

$$|x|^n = |a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \ldots + a_1 x + a_0| \leq \max_{0 \leq i \leq n-1} |a_i x^i| \leq |x|^j$$

for some $0 \leq j \leq n-1$. Hence $|x|^{n-j} \leq 1$, and taking roots $|x| \leq 1$, so $x \in \mathcal{O}_K$.

Moreover $x \in \mathcal{O}_K^\times$ if and only if $x, x^{-1} \in \mathcal{O}_K$, if and only if $|x|, |x|^{-1} \leq 1$, if and only if $|x| = 1$.

Finally $y \in K$ but $y \notin \mathcal{O}_K$ if and only if $|y| > 1$, if and only if $|1/y| < 1$, which implies $y \in \mathcal{O}_K$, and hence K is the field of fractions of $\mathcal{O}_K$.

(ii) If $x, y \in \mathcal{M}_K$, then $|x - y| \leq \max\{\, |x|, |y| \,\} < 1$, so $x - y \in \mathcal{M}_K$. Next if $x \in \mathcal{M}_K$ and $y \in \mathcal{O}_K$, we have $|xy| = |x||y| < 1$, so $xy \in \mathcal{M}_K$. Hence $\mathcal{M}_K$ is an ideal of $\mathcal{O}_K$.

To see that it is maximal, suppose $I \subset \mathcal{O}_K$ is an ideal but $I \not\subset \mathcal{M}_K$. Then there exists some $x \in I \setminus \mathcal{M}_K$, meaning $|x| = 1$, so $x \in \mathcal{O}_K^\times$ is a unit, so $I = \mathcal{O}_K$.

Hence $\mathcal{M}_K$ is the unique maximal ideal of $\mathcal{O}_K$.

(iii) To see that it is a principal ideal domain if $|\cdot|$ is discrete, let $\pi \in \mathcal{M}_K$ such that $|\pi|$ is maximal (which then exists specifically because $|\cdot|$ is discrete).

Suppose $\alpha \in \mathcal{M}_K$, then $|\alpha/\pi| \leq 1$ and so $\alpha/\pi \in \mathcal{O}_K$, whereby $\alpha \in \pi\mathcal{O}_K \subset \mathcal{M}_K$ for every $\alpha \in \mathcal{M}_K$. Now since it's true for all $\alpha \in \mathcal{M}_K$, we indeed have $\mathcal{M}_K = \pi\mathcal{O}_K$.

For any ideal $I \subset \mathcal{O}_K$ the same argument shows that I is generated by some $\alpha \in \mathcal{O}_K$, so $\mathcal{O}_K$ is a principal ideal domain.

Date: March 22nd, 2018.

In fact we can do better: let $n \in \mathbb{N}$ such that $|\alpha/\pi^n| \leq 1$ and $|\alpha/\pi^{n+1}| > 1$, i.e.

$$1 < \left|\frac{\alpha}{\pi^{n+1}}\right| = \frac{1}{|\pi|}\left|\frac{\alpha}{\pi^n}\right|,$$

wherebyh $|\pi| < |\alpha/\pi^n| \leq 1$. Thus $\alpha/\pi^n \in \mathcal{O}_K \setminus \mathcal{M}_K$, so $\alpha/\pi^n \in \mathcal{O}_K^\times$, meaning that $I = \alpha\mathcal{O}_K = \pi^n\mathcal{O}_K = \mathcal{M}_K^\times$, so every ideal is some power of the maximal ideal.

To see that $\mathcal{O}_K$ is a Dedekind domain we need to check three things. First, that it is integrally closed. Second, that it is Noetherian. Thirdly, that it is of dimension 1.

That it is integrally closed we've already established. To be Noetherian is equivalent with having finitely generated ideals, and since $\mathcal{O}_K$ is a principal ideal domain all its ideals are generated by exactly one element.

Finalyl dimension 1 means that all nonzero prime ideals are maximal, and in our case the only nonzero prime ideal is $\mathcal{M}_K$, which is maximal. □

Definition 20.1.3. The ***residue field*** of K is defined as $k = \mathcal{O}_K/\mathcal{M}_K$.

If $|\cdot|$ is discrete, then any $\pi \in \mathcal{O}_K$ such that $\mathcal{M}_K = \pi\mathcal{O}_K$ is called a ***uniformiser*** of $\mathcal{O}_K$.

Definition 20.1.4 (Local field)**.** A ***local field*** is a field which is complete with respect to a discrete non-archimedean valuation such that the residue field is finite.

Remark 20.1.5. Some books instead base the above definition on the topology, i.e. they take K to be a complete locally compact field, in which case the definition inclues $\mathbb{R}$ and $\mathbb{C}$, which the above does not.

Example 20.1.6. Let $K = \mathbb{F}_p(\!(x)\!)$ be the ring of formal Laurent series, i.e. the field of fractions of $\mathbb{F}_p[\![x]\!]$, the ring of formal power series over $\mathbb{F}_p$, with $\mathbb{F}_p$ being the finite field of p elements. Define a valuation on K by $|u| = c^{-r}$ where $c > 1$ and $u = x^r(a_0 + a_1x + \ldots)$ and $a_0 \neq 0$, i.e. r is the order of the series. Then K is a local field with $\mathcal{O}_K = \mathbb{F}_p[\![x]\!]$ and $\mathcal{M}_K = (x)$, and $k = \mathcal{O}_K/\mathcal{M}_K = \mathbb{F}_p$. ▲

Example 20.1.7. Let $K = \mathbb{Q}_p$, with p prime. This is a local field with $\mathcal{O}_K = \mathbb{Z}_p$, the p-adic integers, and $\mathcal{M}_K = p\mathbb{Z}_p$ along with

$$k = \frac{\mathcal{O}_K}{\mathcal{M}_K} = \frac{\mathbb{Z}_p}{p\mathbb{Z}_p} \cong \frac{\mathbb{Z}}{p\mathbb{Z}} = \mathbb{F}_p. \qquad ▲$$

We won't prove the following theorme because it requires delving deeper into the formal Laurent series, but for the record note that

Theorem 20.1.8. *The local fields are preciselt the finite extensions of fields $\mathbb{Q}_p$ or $\mathbb{F}_p(\!(x)\!)$, with p a prime.*

20.2 p-adic Numbers

The p-adic numbers were introduced by Hensel (1861–1941).

For each prime $p \in \mathbb{Z}$, we define a valuation $|\cdot|_p$ on $\mathbb{Q}$ in the following way. For $a \in \mathbb{Q}$, write $a = p^m \cdot b/c$ where $m \in \mathbb{Z}$ and $p \nmid bc$. Then we define $|a|_p = p^{-m}$.

This valuation $|\cdot|_p$ is a nonarchimedean valuation on $\mathbb{Q}$.

Note that the valuation ring is

$$\{\, x \in \mathbb{Q} \mid |x|_p \leq 1 \,\} = \left\{\, \frac{b}{c} \in \mathbb{Q} \;\middle|\; p \nmid c \,\right\} = \mathbb{Z}_{(p)},$$

i.e. the localisation of $\mathbb{Z}$ at $P = (p)$.

Let $\mathbb{Q}_p$ be the completion of $\mathbb{Q}$ with respect to $|\cdot|_p$.

Since this means that $\mathbb{Q}_p$ is composed of equivalence classes of Cauchy sequences in $\mathbb{Q}$, we ask ourselves what the Cauchy sequences in $\mathbb{Q}$ with respect to $|\cdot|_p$ are.

For this we consider the p-adic expansion. First, take $f \in \mathbb{N}$. Then f can be written as

$$f = a_0 + a_1 p + a_2 p^2 + \ldots + a_n p^n$$

with $0 \leq a_i \leq p-1$, i.e. we've written f in base p. If $a_m \neq 0$ and $a_i = 0$ for all $i < m$, i.e. m is the index of the first nonzero coefficient, then $|f|_p = p^{-m}$. As $m \to \infty$, this goes to 0.

Hence for $0 \leq a_i \leq p-1$,

$$\left\{ \sum_{n=0}^{N} a_n p^n \right\}_{N=1}^{\infty}$$

is a Cauchy sequence in $\mathbb{Q}$. Hence this sequence converges in $\mathbb{Q}_p$.

In order to extend this to negative integers, we need a p-adic expansion of -1. To accomplishthis, note that

$$\begin{aligned} -1 &= (p-1) - p = (p-1) + (p-1)p - p^2 \\ &= (p-1) + (p-1)p + (p-1)p^2 - p^3 = \ldots = \sum_{n=0}^{\infty} (p-1)p^n \end{aligned}$$

converges in $\mathbb{Q}_p$.

In this way we can express all integers as p-adic expansions.

For $a = p^m \cdot b/c \in \mathbb{Q}$, $m \in \mathbb{Z}$ and $p \nmid bc$ with $c > 0$, we need to find the p-adic expansion of $1/c$, then multiply by the expansion of $p^m b$.

Note that since $\gcd(p, c) = 1$, we have $p \in (\mathbb{Z}/c\mathbb{Z})^\times$, so $p^k \equiv 1 \pmod{c}$ for some $k \in \mathbb{N}$. Hence $1 - p^k = cd$ for some $d \in \mathbb{Z}$, and so

$$\frac{1}{c} = \frac{d}{cd} = \frac{d}{1-p^k} = d(1 + p^k + p^{2k} + \ldots)$$

by geometric series.

Hence

$$\mathbb{Q}_p = \left\{ \sum_{n \geq m} a_n p^n \;\middle|\; m \in \mathbb{Z},\ 0 \leq a_n \leq p-1 \right\}$$

and

$$\mathbb{Z}_p = \{\, x \in \mathbb{Q}_p \mid |x|_p \leq 1 \,\}$$

is the valuation ring of $\mathbb{Q}_p$, which means

$$\mathbb{Z}_p = \left\{ \sum_{n \geq 0} a_n p^n \;\middle|\; 0 \leq a_n \leq p-1 \right\}.$$

The maximal ideal

$$p\mathbb{Z}_p = \{\, x \in \mathbb{Z}_p \mid |x|_p < 1 \,\} = \Big\{ \sum_{n\geq 1} a_n p^n \;\Big|\; 0 \leq a_n \leq p-1 \Big\}$$

and

$$\mathbb{Z}_p^\times = \Big\{ \sum_{n\geq 0} a_n p^n \;\Big|\; 0 \leq a_n \leq p-1,\ a_0 \neq 0 \Big\}.$$

Finally the residue field

$$k = \frac{\mathbb{Z}_p}{p\mathbb{Z}_p} \cong \frac{\mathbb{Z}}{p\mathbb{Z}} = \mathbb{F}_p,$$

whence $(\mathbb{Q}_p, |\cdot|_p)$ is a local field.

Lecture 21 Hensel's Lemma

21.1 Generalisation of p-adic Numbers

Let $\mathcal{O}$ be any Dedekind domain and $\mathcal{P} \subset \mathcal{O}$ a nonzero prime ideal. Assume $k = \mathcal{O}/\mathcal{P}$ is a finite field.

Let K be the field of fractions of $\mathcal{O}$, and define $|\cdot|_\mathcal{P}$ on K by

$$|x|_\mathcal{P} = (\#k)^{-\operatorname{ord}_\mathcal{P}(x)} = (\mathrm{N}(\mathcal{P}))^{-\operatorname{ord}_\mathcal{P}(x)}$$

for $x \neq 0$, where $\operatorname{ord}_\mathcal{P}(x)$ is the power of $\mathcal{P}$ that appears in the prime factorisation of the ideal (x).

This is a nonarchimedean discrete valuation on K, but it might not be complete.

Example 21.1.1. Take $\mathcal{O} = \mathbb{Z}$ and $K = \mathbb{Q}$, along with $\mathcal{P} = p\mathbb{Z}$. ▲

Take $\pi \in \mathcal{P} \setminus \mathcal{P}^2$. Then $\operatorname{ord}_\mathcal{P}(\pi) = 1$ so $|\pi|_\mathcal{P} = (\#k)^{-1}$.

Let R be the set of representatives for $\mathcal{O}/\mathcal{P}$, a finite set.

The valuation ring of K with respect to $|\cdot|_\mathcal{P}$ is

$$\{\, x \in K \mid |x|_\mathcal{P} \leq 1 \,\} = \{\, x \in K \mid \operatorname{ord}_\mathcal{P}(x) \geq 0 \,\}.$$

The element π is a uniformiser of this ring, and $\mathcal{M} = (\pi)$ is the maximal ideal.

Let $K_\mathcal{P}$ be the completion of K with respect to $|\cdot|_\mathcal{P}$. Then

$$\mathcal{O}_{K_\mathcal{P}} = \Big\{ \sum_{n\geq 0} r_n \pi^n \;\Big|\; r_n \in R \Big\}$$

and

$$K_\mathcal{P} = \Big\{ \sum_{n\geq m} r_n \pi^n \;\Big|\; r_n \in R,\ m \in \mathbb{Z} \Big\}.$$

In addition $\mathcal{M}_{K_\mathcal{P}} = \pi\mathcal{O}_{K_\mathcal{P}}$ is the maximal ideal of $\mathcal{O}_{K_\mathcal{P}}$.

The residue field is

$$\frac{\mathcal{O}_{K_\mathcal{P}}}{\mathcal{M}_{K_\mathcal{P}}} \cong \frac{\mathcal{O}}{\mathcal{P}} = k.$$

Then $K_\mathcal{P}$ is called a ***$\mathcal{P}$-adic field***.

Remark 21.1.2. Let L be a local field. Set $K_\mathcal{P} = L$ with $\mathcal{P} = \mathcal{M}_L$, the unique maximal ideal. Thus every local field is a $\mathcal{P}$-adic field.

Date: March 27th, 2018.

21.2 Topology of Local Fields

Let K be a local field and $\mathcal{O}_K = \{ x \mid |x| \leq 1 \}$ its valuation ring.

Lemma 21.2.1. *The valuation ring $\mathcal{O}_K$ is compact.*

Proof. First we note that $\mathcal{O}_K$ is both open and closed. This is because $\varphi = |\cdot| \colon K \to \mathbb{R}$ is a continuous map, so

$$\mathcal{O}_K = \varphi^{-1}([0,1])$$

is closed since $[0,1]$ is closed in $\mathbb{R}$. But on the other hand

$$\mathcal{O}_K = \varphi^{-1}((-\delta, 1+\delta))$$

for some $\delta > 0$ since $|\cdot|$ is discrete, and this set is open.

Secondly, $\mathcal{O}_K$ is complete as a metric space with respect to $|\cdot|$.

If $\{ x_n \} \subset \mathcal{O}_K$ is Cauchy, then $x_n \to x$ in K. Since $\mathcal{O}_K$ is closed, we moreover have $x \in \mathcal{O}_K$.

A metrix space X is compact if and only if it is complete and ***totally bounded***, i.e. for any $\varepsilon > 0$ the space X is covered by finitely many ε-balls.

Note that $\mathcal{O}_K$ has a unique maximal ideal $\mathcal{M}_K = (\pi)$ with $|\pi| < 1$. Given any $\varepsilon > 0$, take $n \in \mathbb{N}$ such that $|\pi|^n < \varepsilon$.

Then

$$\left| \frac{\mathcal{O}_K}{\pi^n \mathcal{O}_K} \right| = (\#k)^n < \infty,$$

and let $x_1, x_2, \ldots, x_m \in \mathcal{O}_K$ be the representatives of $\mathcal{O}_K / \pi^n \mathcal{O}_K$.

We claim that

$$\mathcal{O}_K = \bigcup_{i=1}^{n} B_\varepsilon(x_i)$$

with $B_\varepsilon(x) = \{ a \in \mathcal{O}_K \mid |a - x| < \varepsilon \}$.

For any $a \in \mathcal{O}_K$, in the quotient $\mathcal{O}_K / \pi^n \mathcal{O}_K$ we have

$$a = x_i + \pi^n b$$

for some i and some $b \in \mathcal{O}_K$. Then

$$|a - x_i| = |\pi^n| b \leq |\pi|^n < \varepsilon$$

so $a \in B_\varepsilon(x_i)$.

Hence $\mathcal{O}_K$ is totally bounded, which along with $\mathcal{O}_K$ being complete hence means that it is compact. □

Corollary 21.2.2. *Let K be a local field and $A \subset K$ a subset. Then A is compact if and only if A is closed and bounded.*

That is to say, local fields behave somewhat like Euclidean spaces.

Proof. For the forward direction, A being compact implies A is complete, meaning that it is closed. Moreover $|\cdot| \colon K \to \mathbb{R}$ is continuous, so since $|A| \subset \mathbb{R}$ is compact, hence closed and bounded, $|A| < C$ for some $C \in \mathbb{R}$.

For the reverse direction, assume A is closed and bounded, i.e. $|A| < C$ for some $C > 0$. Take any $z \in K$ such that $|z| > C$ (this must exist because if

$|z| > 1$ we raise it to some big power, and if $|z| < 1$ we raise its inverse to some big power). Then $|a| < |z|$ for all $a \in A$, hence $|a/z| < 1$, i.e. $z^{-1}A \subset \mathcal{O}_K$, so $z^{-1}A$ is a closed subset of a compact set, meaning it's compact, and therefore A is compact. □

Corollary 21.2.3. *Let K be a local field. Then K is locally compact (i.e. every element has a compact neighbourhood) and each fractional ideal of K is compact.*

21.3 Hensel's Lemma

Recall how if $|\cdot|$ is a nonarchimedean valuations on a field K that is complete with respect $|\cdot|$, we have

$$|x + y| \leq \max\{\, |x|, |y| \,\}$$

and if $|x| < |y|$¡ then $|x + y| = |y|$.

To see this, note that $|x| < |y|$ implies $|x/y| < 1$, so $x/y \in \mathcal{M}_K$, whence $1 + x/y \in \mathcal{O}_K^\times$. Hence $|1 + x/y| = 1$, and multiplying by $|y|$ we get $|x + y| = |y|$.

Theorem 21.3.1 (Hensel's lemma, first form)**.** *Let K be a field complete with respect to a nonarchimedean valuation $|\cdot|$. Ket $f(x) \in \mathcal{O}_K[x]$. Suppose there exists $\alpha_0 \in \mathcal{O}_K$ such that $|f(\alpha_0)| < |f'(\alpha_0)|^2$. Then there exists a unique $\alpha \in \mathcal{O}_K$ such that*

(*i*) $f(\alpha) = 0$ *and*

(*ii*) $|\alpha - \alpha_0| \leq \left|\dfrac{f(\alpha_0)}{f'(\alpha_0)^2}\right|$.

Proof. The proof essentially boils down to Newton's method from first semester calculus. Consider the sequence

$$\alpha_{i+1} = \alpha_i - \frac{f(\alpha_i)}{f'(\alpha_i)}$$

for $i = 0, 1, 2, \ldots$. Let

$$C = \left|\frac{f(\alpha_0)}{f'(\alpha_0)^2}\right| < 1$$

by assumption. We will show inductively that

(*i*) $|\alpha_i| \leq 1$, i.e. $\alpha_i \in \mathcal{O}_K$;

(*ii*) $|\alpha_i - \alpha_0| \leq C$;

(*iii*) $\left|\dfrac{f(\alpha_i)}{f'(\alpha_i)^2}\right| \leq C^{2^i}$.

The case $i = 0$ is true by assumptions in the theorem. Assume then that it is true for i, and consider $i + 1$. We then have

$$|\alpha_{i+1} - \alpha_i| = \left|\frac{f(\alpha_i)}{f'(\alpha_i)}\right| \leq \left|\frac{f(\alpha_i)}{f'(\alpha_i)^2}\right| \leq C^{2^i} < 1$$

since $f(x) \in \mathcal{O}_K[x]$ implies $f'(x) \in \mathcal{O}_K[x]$, whence $f'(\alpha_i) \in \mathcal{O}_K$ and so $|f'(\alpha_i)| \leq 1$ and hence $1/|f'(\alpha_i)| \geq 1$. Therefore

$$|\alpha_{i+1}| \leq \max\{\, |\alpha_{i+1} - \alpha_i|, |\alpha_i| \,\} \leq 1,$$

ticking off the first property.

For the second property,

$$|\alpha_{i+1} - \alpha_0| \leq \max\{\, |\alpha_{i+1} - \alpha_i|, |\alpha_i - \alpha_0| \,\} \leq C$$

since the first is bounded by $C^{2^i} \leq C$ by what we did above, and $|\alpha_i - \alpha_0| \leq C$ by our inductive hypothesis.

Finally let $f_j(x) \in \mathcal{O}_K[x]$ be define dby

$$f(x+y) = f(x) + f_1(x)y + f_2(x)y^2 + \ldots + f_k(x)y^k;$$

then $f_1(x) = f'(x)$—think Taylor expansions.

Hence

$$f(\alpha_{i+1}) = f\Big(\alpha_i - \frac{f(\alpha_i)}{f'(\alpha_i)}\Big) = f(\alpha_i) + f'(\alpha_i)\Big(-\frac{f(\alpha_i)}{f'(\alpha_i)}\Big) + \beta\Big(\frac{f(\alpha_i)}{f'(\alpha_i)}\Big)^2,$$

where $\beta \in \mathcal{O}_K$. The first two terms make 0, so

$$|f(\alpha_{i+1})| \leq \Big|\frac{f(\alpha_i)}{f'(\alpha_i)}\Big|^2.$$

Now do the same with f_1, i.e.

$$f_1(x+y) = f_1(x) + g_1(x)y + g_2(x)y^2 + \ldots + g_\ell(x)y^\ell,$$

with $g_i(x) \in \mathcal{O}_K[x]$. Then

$$f_1(\alpha_{i+1}) = f_1\Big(\alpha_i - \frac{f(\alpha_i)}{f'(\alpha_i)}\Big) = f_1(\alpha_1) + \gamma\frac{f(\alpha_i)}{f'(\alpha_i)},$$

with $\gamma \in \mathcal{O}_K$.

Therefore

$$\frac{f'(\alpha_{i+1})}{f'(\alpha_i)} = 1 + \gamma\frac{f(\alpha_i)}{f'(\alpha_i)^2}.$$

Note that

$$\Big|\gamma\frac{f(\alpha_i)}{f'(\alpha_i)^2}\Big| \leq 1 \cdot C^{2^i} < 1,$$

so

$$\Big|\frac{f'(\alpha_{i+1})}{f'(\alpha_i)}\Big| = 1,$$

the maximum of the above sum, whereby $|f'(\alpha_{i+1})| = |f'(\alpha_i)|$.

Finally

$$\Big|\frac{f(\alpha_{i+1})}{f'(\alpha_{i+1})^2}\Big| \leq \Big|\frac{f(\alpha_i)}{f'(\alpha_i)}\Big|^2 \frac{1}{|f'(\alpha_i)^2|} = \Big|\frac{f(\alpha_i)}{f'(\alpha_i)^2}\Big|^2 \leq (C^{2^i})^2 = C^{2^{i+1}}.$$

Using this we can finish the proof of the theorem, since from the third property

$$|\alpha_{i+1} - \alpha_i| = \left|\frac{f(\alpha_i)}{f'(\alpha_i)}\right| \leq \left|\frac{f(\alpha_i)}{f'(\alpha_i)^2}\right| \leq C^{2^i} \to 0$$

as $i \to \infty$ since $C < 1$. Hence $|\alpha_i|$ is Cauchy in $\mathcal{O}_K$ since $|\cdot|$ is nonarchimedean (meaning that subsequent terms going to zero is enough for Cauchy). Ergo $\alpha_i \to \alpha$, with $\alpha \in \mathcal{O}_K$, and by the second property $|\alpha - \alpha_0| < C$, whence by the third property

$$|f(\alpha_i)| \leq |f'(\alpha_i)|^2 C^{2^i}.$$

Taking the limit as $i \to \infty$, this goes to $|f(\alpha)| = 0$, meaning that $f(\alpha) = 0$. □

Corollary 21.3.2. *Let K be a field complete with respect to a nonarchimedean valuation $|\cdot|$. Suppose $f(x) \in \mathcal{O}_K[x]$ and $\alpha_0 \in \mathcal{O}_K$ such that $f(\alpha_0) \equiv 0 \pmod{\mathcal{M}_K}$ and $f'(\alpha_0) \not\equiv 0 \pmod{\mathcal{M}_K}$. Then there exists $\alpha \in \mathcal{O}_K$ such that $f(\alpha) = 0$ and $\alpha \equiv \alpha_0 \pmod{\mathcal{M}_K}$.*

Proof. The assumptions give $|f(\alpha_0)| < 1$ since $f(\alpha_0) \in \mathcal{M}_K$, and $|f'(\alpha_0)| = 1$ since it's in $\mathcal{O}_K$ but not in $\mathcal{M}_K$. So we can apply Hensel's lemma. □

This means that the existence of solutions to polynomial equations becomes easy in local fields—we need only check finitely many places.

Lecture 22 Hensel's Lemma revisited

22.1 Second Form of Hensel's Lemma

Theorem 22.1.1 (Hensen's lemma, second form)**.** *Let K be a field complete with respect to a nonarchimedean discrete*[1] *valuation $|\cdot|$.*

Let $f(x) \in \mathcal{O}_K[x]$ be a monic polynomial and let $k = \mathcal{O}_K/\mathcal{M}_K$ be the residue field of K.

Suppose $\bar{h}, \bar{y} \in k[x]$ such that $f(x) \equiv \bar{h}(x)\bar{g}(x) \pmod{\mathcal{M}_K}$ in $k[x]$ and $\gcd(\bar{h}, \bar{g}) = 1$. Then there exists $h(x), g(x) \in \mathcal{O}_K[x]$ such that $f(x) = h(x)g(x)$ and $h(x) \equiv \bar{h}(x) \pmod{\mathcal{M}_K}$ and $g(x) \equiv \bar{g}(x) \pmod{\mathcal{M}_K}$.

Moreover $g(x)$ and $h(x)$ are unique up to multiplication by scalar.

Proof. Let $\mathcal{M}_K = (\pi)$ (note that $\mathcal{O}_K$ is a discrete valuation ring and hence a principal ideal domain since $|\cdot|$ is discrete; otherwise we would take $\pi \in \mathcal{M}_K \setminus \mathcal{M}_K^2$).

We start by proving existence. For $n \geq 0$ we will construct, inductively, $g_n(x), h_n(x) \in \mathcal{O}_K[x]$ with leading coefficients being units such that

$$f(x) - g_n(x)h_n(x) \equiv 0 \pmod{(\pi^{n+1})},$$

along with $g_n(x) \equiv \bar{g}(x) \pmod{\pi}$, $h_n(x) \equiv \bar{h}(x) \pmod{\pi}$ and $g_n(x) \equiv g_{n+1}(x) \pmod{\pi^n}$ and $h_n(x) \equiv h_{n-1}(x) \pmod{\pi^n}$.

For $n = 0$, let $g_0(x)$ and $h_(x)$ be any lifts of $\bar{g}(x)$ and $\bar{h}(x)$ in $\mathcal{O}_K[x]$.

Date: March 29th, 2018.

[1]The assumption of $|\cdot|$ being discrete is not essential, but simplifies the proof.

For $n > 0$, suppose we have $g_{n-1}(x)$ and $h_{n-1}(x)$ constructed. Let

$$p(x) = \frac{f(x) - g_{n-1}(x)h_{n-1}(x)}{\pi^n} \in \mathcal{O}_K[x]$$

by the inductive hypothesis. Since $\gcd(\bar{g}, \bar{h}) = 1$ in $k[x]$ there exists some $u_n(x)$ and $v_n(x)$ in $\mathcal{O}_K[x]$ such that

$$u_n(x)g_{n-1}(x) + v_n(x)h_{n-1}(x) \equiv p(x) \pmod{\pi}.$$

Put

$$g_n(x) = g_{n-1}(x) + \pi^n v_n(x) \in \mathcal{O}_K[x]$$

and

$$h_n(x) = h_{n-1}(x) + \pi^n u_n(x) \in \mathcal{O}_K[x].$$

Then $h_n(x) \equiv h_{n-1}(x) \pmod{\pi^n}$ and $g_n(x) \equiv g_{n-1}(x) \pmod{\pi^n}$, and $g_n(x) \equiv \bar{g}(x) \pmod{\pi}$ and $h_n(x) \equiv \bar{h}(x) \pmod{\pi}$ as well.

Then

$$\begin{aligned} f(x) - g_n(x)h_n(x) &= f(x) - \big(g_{n-1}(x) + \pi^n v_n(x)\big)\big(h_{n-1}(x) + \pi^n u_n(x)\big) \\ &= \underbrace{f(x) - g_{n-1}(x)h_{n-1}(x)}_{= p(x)\pi^n} - \pi^n\big(u_n(x)g_{n-1}(x) + v_n(x)h_{n-1}(x)\big) \\ &\equiv p(x)\pi^n - \pi^n p(x) \equiv 0 \pmod{\pi^{n+1}}. \end{aligned}$$

since the second part of the middle line is $p(x) + \pi w(x)$ for some $w(x) \in \mathcal{O}_K[x]$.

Hence

$$|g_n(x) - g_{n-1}(x)| < |\pi|^k \to 0$$

and

$$|h_n(x) - h_{n-1}(x)| < |\pi|^k \to 0$$

as $n \to \infty$, meaning that $\{\, g_n(x) \,\}$ and $\{\, h_n(x) \,\}$ are Cauchy in $\mathcal{O}_K[x]$, so they approach some $g(x), h(x) \in \mathcal{O}_K[x]$ such that $f(x) = g(x)h(x)$ and $g \equiv \bar{g} \pmod{\pi}$ and $h \equiv \bar{h} \pmod{\pi}$.

Next let us prove uniqueness. Since $\gcd(\bar{g}, \bar{h}) = 1$ in $k[x]$, we have that the ideal $(\bar{g}, \bar{h}) = k[x]$, meaning that

$$(g, h) + \mathcal{M}_K\mathcal{O}_K[x] = \mathcal{O}_K[x]$$

for any lifts of $\bar{g}$ and $\bar{h}$. Let $M = \mathcal{O}_K[x]/(g, h)$, which is an $\mathcal{O}_K$-module.

Note that the Jacobson radical (i.e. the intersection of all maximal ideals) of $\mathcal{O}_K$ is $\mathcal{M}_K$ since there is only one maximal ideal. Now $\mathcal{M}_K M = M$ by the above, whence by Nakayama's lemma we must have $M = 0$. Hence $(g, h) = \mathcal{O}_K[x]$, so any lifts are coprime.

Now suppose $f(x) = g(x)h(x) = g_1(x)h_1(x)$ in $\mathcal{O}_K[x]$, so that $g \equiv g_1 \equiv \bar{g} \pmod{\pi}$ and $h \equiv h_1 \equiv \bar{h} \pmod{\pi}$. Then since any two lifts are coprimne, $(g_1, h) = \mathcal{O}_K[x]$, and so there exists $r(x), s(x) \in \mathcal{O}_K[x]$ such that $r(x)g_1(x) + s(x)h(x) = 1$.

Thus

$$h_1(x) = h_1(x)(r(x)g_1(x) + s(x)h(x))$$

which we can distribute and switch $h_1(x)g_1(x)$ for $h(x)g(x)$ so

$$h_1(x) = r(x)g(x)h(x) + h_1(x)s(x)h(x) = h(x)(r(x)g(x) + h_1(x)s(x))$$

meaning that $h(x) \mid h_1(x)$ in $\mathcal{O}_K[x]$. Repeating the same argument with the roles of $h(x)$ and $h_1(x)$ switched we get $h_1(x) \mid h(x)$, so $h(x) = uh_1(x)$ for some unit $u \in \mathcal{O}_K^\times$.

The exact same argument applies to $g(x)$. □

22.2 Extension of Valuations

Theorem 22.2.1. *Suppose K is a field complete with respect to a discrete nonarchimedean valuation $|\cdot|$. Suppose L is a finite separable extension of K (note that it is unnecessary to assume separability if we are in characteristic 0 since every algebraic extension of a field of characteristic 0 is separable).*

Then we have

(*i*) *There exists a unique valuation $|\cdot|_L$ on L extending $|\cdot|$, and $|\cdot|_L$ is discrete and nonarchimedean.*

(*ii*) *The valuation ring $\mathcal{O}_L$ of $|\cdot|_L$ is the integral closure of $\mathcal{O}_K$ in L.*

(*iii*) *For $\beta \in L$, $|\beta|_L = |\mathrm{N}_{L/K}(\beta)|^{1/n}$, where $n = [L : K]$.*

(*iv*) *L is complete with respect to $|\cdot|_L$.*

(*v*) *If K is local, then L is local.*

Proof. Let π be a uniformiser of K, i.e. $\mathcal{M}_K = (\pi)$. Let $\mathcal{O}_L$ be the integral closure of $\mathcal{O}_K$ in L.

First we note that $\mathcal{O}_L$ is a Dedekind domain and a finite rank free $\mathcal{O}_K$-module. The proof of this is identical to the proof of $\mathcal{O}_K$ being the same when K is a number field, and bouls down to $\mathcal{O}_K$ (respectively $\mathcal{O}_L$) being a principal ideal domain.

Secondly, $\mathcal{O}_L$ has a unique maximal ideal. To see this, let $\mathcal{M}_L$ be any maximal ideal in $\mathcal{O}_L$. Then since $\mathcal{O}_L$ is integral over $\mathcal{O}_K$, $\mathcal{M}_L \cap \mathcal{O}_K$ is a maximal ideal in $\mathcal{O}_K$, so $\mathcal{M}_L \cap \mathcal{O}_K = \mathcal{M}_K$. In particular all maximal ideals in $\mathcal{O}_L$ appear in the factorisation of $\mathcal{M}_K\mathcal{O}_L$, whence

$$\mathcal{M}_K\mathcal{O}_L = \mathcal{M}_1^{s_1}\mathcal{M}_2^{s_2}\cdots\mathcal{M}_r^{s_r},$$

where $\mathcal{M}_i$ are all maximal ideals in $\mathcal{O}_L$ and $s_i > 0$ for all i. Hence

$$\frac{\mathcal{O}_L}{\mathcal{M}_K\mathcal{O}_L} = \bigoplus_{i=1}^{r} \frac{\mathcal{O}_L}{\mathcal{M}_i^{s_i}}$$

by the Chinese remainder theorem. Suppose $r \geq 2$ and let $e_1 = (1, 0, \ldots, 0)$ and $e_2 = (0, 1, 0, \ldots, 0)$ above. Then choose $\alpha \in \mathcal{O}_L$ such that $\alpha \mapsto e_1 + e_2$ in the direct sum, and let $f(x) \in \mathcal{O}_K[x]$ be the monic minimal polynomial of α over K.

Then we have

$$\begin{array}{ccccccccc}
\frac{\mathcal{O}_K}{(f(x))} & \xrightarrow{\cong} & \mathcal{O}_K[x] & \hookrightarrow & \mathcal{O}_L & \longrightarrow & \frac{\mathcal{O}_L}{\mathcal{M}_K\mathcal{O}_L} & \longrightarrow & \bigoplus_{i=1}^{2} \frac{\mathcal{O}_L}{\mathcal{M}_i^{s_i}} \\
x & \longmapsto & \alpha & \longmapsto & \alpha & \longmapsto & \bar{\alpha} & \longmapsto & (1,1) \\
 & & \frac{\mathcal{O}_K[x]}{(\mathcal{M}_K, f(x))} & \cong & \frac{k[x]}{(\bar{f}(x))} & & & & \\
 & & \bar{x} & \longmapsto & & & & & \bar{\alpha}
\end{array}$$

This implies $\bar{f}(x)$ has nontrivial coprime factors in $k[x]$ since things split at the end of the diagram. In other words, $\bar{f}(x) \equiv \bar{g}(x)\bar{h}(x) \pmod{\mathcal{M}_K}$ with $\gcd(\bar{g}, \bar{h}) = 1$ in $k[x]$.

By Hensel's lemma therefore $f(x) = g(x)h(x)$ in $\mathcal{O}_K[x]$, which is a contradiction since f is irreducible in $\mathcal{O}_K[x]$, being the minimal polynomial of α over K. Hence $r = 1$, i.e. there is only one maximal ideal in $\mathcal{O}_L$.

Thirdly, $|\cdot|$ extends to a discrete valuation on L. To see this, let $\mathcal{M}_L$ be the unique maximal ideal on $\mathcal{O}_L$. By the Chinese remainder theorem any Dedekind domain with a finite number of primes is a principal ideal domain, so $\mathcal{M}_L = (\omega)$.

Suppose $\mathcal{M}_K\mathcal{O}_L = \mathcal{M}_L^e = (\omega)^e$. For $x \in L$, define $|x|_L = |\pi|^{\operatorname{ord}_{\mathcal{M}_L}(x)/e}$, where $\mathcal{M}_K = \pi\mathcal{O}_K$. So $x\mathcal{O}_L = \mathcal{M}_L^{\operatorname{ord}_{\mathcal{M}_L}(x)}$.

This gives a discrete nonarchimedean valuation on L. Moreover $|\pi|_L = |\pi|^{e/e} = |\pi|$, meaning that $|\cdot|_L$ agrees with $|\cdot|$ on K.

Fourthly, for $\beta \in L$, $|\beta|_L = |\mathrm{N}_{L/K}(\beta)|^{1/n}$. To show this it suffices to show that this is true for $\beta = \omega$.

Note that $\mathrm{N}_{L/K}(\omega) = \pi^f \cdot u$, where $f = f(\mathcal{M}_L/\mathcal{M}_K)$ is the inertial degree, and $u \in \mathcal{O}_K^\times$ since $(\pi) = (\omega)^e$, with $\pi = \omega^e \cdot u$ and $fe = n$.

Then

$$\pi^n = \mathrm{N}(\pi) = \mathrm{N}(\omega)^e \,\mathrm{N}(u),$$

with the norm of u being in $\mathcal{O}_K^\times$, so $\mathrm{N}(\omega) = \pi^{n/e}$.

Hence

$$|\mathrm{N}_{L/K}(\omega)|^{1/n} = |\pi^f u|^{1/(fe)} = |\pi|^{1/e} = |\pi|^{\operatorname{ord}_{\mathcal{M}_L}(\omega)/e} = |\omega|_L.$$

□

Lecture 23 Krasner's Lemma

23.1 Proof continued

We start by finishing up the proof from last time.

Proof continued. Step five: Show that $\mathcal{O}_L$ is the valuation ring of $|\cdot|_L$.

Suppose $x \in L$ with $|x|_L \leq 1$. If $x \notin \mathcal{O}_L$, then $x = \omega^r \cdot u$ with $r < 0$ and $u \in \mathcal{O}_L^\times$. Then

$$|x|_L = |\omega|_L^r = |\pi|^{r/e} > 1$$

since $|\pi| < 1$ and $r < 0$. This is a contradiction; $|x|$ can't simultaneously be less than or equal to 1 and greater than 1.

Hence $x \in \mathcal{O}_L$ if and only if $|x|_L \leq 1$, meaning that x is in the valuation ring of L with respect to $|\cdot|_L$.

It remains to show that $|\cdot|_L$ is the unique extension of $|\cdot|$ and that L is complete with respect to $|\cdot|_L$.

Step six: Show that L is complete with respect to $|\cdot|_L$.

Let $\{\alpha_N\}$ be a Cauchy sequence in L, and let $e_1, e_2, \ldots, e_n$ be an $\mathcal{O}_K$-basis of $\mathcal{O}_L$ (since it is a finite rank free $\mathcal{O}_K$-module), and hence also a K-basis for L.

Date: April 3rd, 2018.

Write

$$\alpha_N = \beta_{N,1}e_1 + \beta_{N,2}e_2 + \ldots + \beta_{N,n}e_n$$

with $\beta_{N,i} \in K$. Then for each $r > 0$ there exists some $M \in \mathbb{N}$ such that for every $N, N' \geq M$ we have

$$|\alpha_N - \alpha_{N'}| < |\pi|^r < 1$$

since the sequence if Cauchy. Therefore $\alpha_N - \alpha_{N'} \in \pi^r \mathcal{O}_L$, meaning that $\beta_{N,i} - \beta_{N',i} \in \pi^r \mathcal{O}_K$ since the e_i are linearly independent.

Hence $|\beta_{N,i} - \beta_{N',i}| < |\pi|^r$, so $\{\, \beta_{N,i} \,\}$ is Cauchy in K, and K is complete with respect to $|\cdot|$, so $\beta_{N,i} \to \beta_i$ in K.

Hence let

$$\alpha = \beta_1 e_1 + \beta_2 e_2 + \ldots + \beta_n e_n$$

and $\alpha_N \to \alpha$ in L.

Step seven: Show that if $\|\cdot\|$ is an extension of $|\cdot|$ to L, then if $x \in \mathcal{O}_L$, we must have $\|x\| \leq 1$. In particular if $x \in \mathcal{O}_L^\times$, then $\|x\| = 1$.

To see this, write

$$\mathcal{O}_L = \mathcal{O}_K e_1 \oplus \mathcal{O}_K e_2 \oplus \ldots \oplus \mathcal{O}_K e_n.$$

Take $r > 0$ such that

$$(\|e_1\| + \|e_2\| + \ldots + \|e_n\|)^r \leq 2.$$

Then for $x \in \mathcal{O}_L$, write $x = \beta_1 e_1 + \beta_2 e_2 + \ldots + \beta_n e_n$ with $\beta_i \in \mathcal{O}_K$. Then by the triangle inequality

$$\|x\|^r \leq (\|\beta_1\|\|e_1\| + \|\beta_2\|\|e_2\| + \ldots + \|\beta_n\|\|e_n\|)^r \leq (\|e_1\| + \|e_2\| + \ldots + \|e_n\|)^r \leq 2,$$

since $\|\beta_1\| = |\beta_1|$ due to $\|\cdot\|$ being an extension of $|\cdot|$, and hence $\|\beta_1\| \leq 1$, and likewise for β_2 and so forth.

Thus $\|x\| \leq 2^{1/r}$ is uniformly bounded, meaning that if there exists $x \in \mathcal{O}_L$ such that $\|x\| > 1$, then $\|x^n\| \to \infty$, which would contradict the uniform bound.

Hence $\|x\| \leq 1$ for all $x \in \mathcal{O}_L$, and the unit property follows.

Finally, step eight: Show that $|\cdot|_L$ is unique. To do this, suppose $\|\cdot\|$ is an extension of $|\cdot|$ to L alongside $|\cdot|_L$.

It suffices to show that they agree on ω, a uniformiser for $\mathcal{O}_L$, i.e. $\|\omega\| = |\omega|_L$. Write $\pi = \omega^e \cdot u$, with $u \in \mathcal{O}_L^\times$ and $e = e(\mathcal{M}_L/\mathcal{M}_K)$. Then

$$\|\omega\|^e = \|\pi\| = abs\pi = |\omega|_L^e,$$

meaning that $\|\omega\| = |\omega|_L$. □

Corollary 23.1.1. *Suppose K is a field complete with respect to a discrete non-archimedean valuation $|\cdot|$. If L is any separable algebraic extension of K (not necessarily finite), then $|\cdot|$ extends uniquely to a non-archimedean valuation on L.*

Proof. Since L is the union of finite extensions of K, we can apply the previous theorem step by step. □

Remark 23.1.2. The extension of valuations might not be discrete in the infinite extension case, and L might not be complete with respect to the extended valuation in this situation either.

Example 23.1.3. Consider $(\mathbb{Q}_p, |\cdot|_p)$, and let $\overline{\mathbb{Q}_p}$ be its algebraic closure. Then $(\overline{\mathbb{Q}_p}, |\cdot|_p)$ is neither discrete nor complete. ▲

Corollary 23.1.4. *Let K be a field complete with respect to a discrete non-archimedean valuation. Let L be a finite separable extension of K, and let $\sigma\colon L \to L^{sep}$ be a K-embedding, where by $L^{sep} = K^{sep}$ we mean the separable closure of L. Then for $\alpha \in L$ we have*

$$|\alpha|_{L^{sep}} = |\sigma(\alpha)|_{L^sep}.$$

Hence if $\alpha \in K^{sep}$ and $\sigma \in \mathrm{Gal}(K^{sep}/K)$, then

$$|\alpha|_{K^{sep}} = |\sigma(\alpha)|_{K^{sep}},$$

so all Galois conjugates have the same valuation.

23.2 Krasner's Lemma

Lemma 23.2.1 (Krasner)**.** *Let K be a field complete with respect to a discrete non-archimedean valuation $|\cdot|$. Suppose $\alpha, \beta \in K^{sep}$ such that*

$$|\alpha - \beta|_{K^{sep}} < |\alpha - \sigma(\alpha)|_{K^{sep}}$$

for every $\sigma \in \mathrm{Gal}(K^{sep}/K)$ with $\sigma(\alpha) \neq \alpha$, i.e. β is closer to α than all of its Galois conjugates. Then $K(\alpha) \subset K(\beta)$.

Proof. It suffices to show $K(\alpha, \beta) = K(\beta)$. Note that we of course know $K(\alpha, \beta) \supset K(\beta)$ out of the box. Suppose therefore that $K(\alpha, \beta) \supsetneq K(\beta)$.

Then there exists some $\sigma \in \mathrm{Gal}(K^{sep}/K)$ such that $\sigma(\beta) = \beta$ but $\sigma(\alpha) \neq \alpha$.

Then since Galois conjugates have the same valuation, as shown above, we have

$$|\alpha - \beta|_{K^{sep}} = |\sigma(\alpha - beta)|_{K^{sep}} = |\sigma(\alpha) - \sigma(\beta)|_{K^{sep}} = |\sigma(\alpha) - \beta|_{K^{sep}}.$$

Thus by the strong triangle inequality

$$\begin{aligned} |\alpha - \sigma(\alpha)|_{K^{sep}} &= |(\alpha - \beta) + (\beta - \sigma(\alpha))|_{K^{sep}} \\ &\leq \max\{\, |\alpha - \beta|_{K^{sep}}, |\beta - \sigma(\alpha)|_{K^{sep}} \,\} = |\alpha - \beta|_{K^{sep}}, \end{aligned}$$

which contradicts the assumption of β being closer to α than all of its Galois conjugates.

Hence $K(\alpha, \beta) = K(\beta)$. □

Definition 23.2.2. Let K be a field complete with respect to a discrete non-archimedean valuation $|\cdot|$. Let $\alpha, \beta \in K^{sep}$. We say that β ***belongs to*** α if

$$|\alpha - \beta|_{K^{sep}} < |\sigma(\alpha) - \alpha|_{K^{sep}}$$

for all $\sigma \in \mathrm{Gal}(K^{sep}/K)$ such that $\sigma(\alpha) \neq \alpha$.

Proposition 23.2.3. *Let K be a field complete with respect to a discrete, non-archimedean valuation $|\cdot|$. Let*

$$f(x) = x^n + a_1 x^{n-1} + \ldots + a_{n-1}x + a_n \in K[x]$$

be separable and irreducible. Let α be a root of $f(x)$.

Then there exists a constant $C(f) > 0$ such that if $g(x) \in K[x]$ is a monic polynomial wuch that

$$\|g(x) - f(x)\| \leq C(f)$$

where for $h(x) = c_m x^m + c_{m-1}x^{m-1} + \ldots + c_1 x + c_0$ we define

$$\|h(x)\| = \max_{0 \leq i \leq m} |c_i|,$$

i.e. the largest coefficient.

Then $g(x)$ has a root β that belongs to α. Moreover $g(x)$ is irreducible and $\deg g = \deg f$, so $K(\alpha) = K(\beta)$.

Proof. Take $C(f) > 0$ such that

(*i*) $C(f) < \min\{\, 1, \|f\| \,\}$, where $\|f\| \neq 0$ since at least one coefficient, the leading one, is 1.

(*ii*) $C(f) < \min\limits_{\sigma(\alpha) \neq \alpha} \{\, \|f\|^{-n} |\sigma(\alpha) - \alpha|^n \,\}$.

Since $C(f) < 1$ and f and g are both monic, we must have $\deg f = \deg g$ since otherwise the biggest coefficients in $f - g$ would be 1, making $\|f(x) - g(x)\| = 1$.

Note that

$$\|g\| \leq \max\{\, \|f\|, \|f - g\| \,\} \leq \|f\|.$$

Write

$$g(x) = x^n + b_1 x^{n-1} + \ldots + b_n.$$

If β_0 is any root of $g(x)$, then

$$|\beta_0|^n = \left| \sum_{i=1}^{n} b_i \beta_0^{n-i} \right| \leq \max_i |b_i| {\beta_0}^{n-i} = |b_j| |\beta_0|^{n-j}$$

if we call j the index that maximises this. Then $|\beta_j| \leq \|g\| \leq \|f\|$, whence the above is less than or equal to $\|f\| |\beta_0|^{n-j}$.

Rearranging, we have

$$|\beta_0|^j \leq \|f\|.$$

Note moreover that since $g(\beta_0) = 0$,

$$\begin{aligned} |f(\beta_0)| = |(f-g)(\beta_0)| &\leq C(f) \max_{1 \leq m \leq n} |\beta_0|^m \leq C(f) \max_{1 \leq m \leq n} \|f\|^{m/j} \\ &< \|f\|^{-n} |\sigma(\alpha) - \alpha|^n \max_{1 \leq m \leq n} \|f\|^{m/j} \leq |\sigma(\alpha) - \alpha|^n \end{aligned}$$

since $m/j - n < 0$ and $\|f\| \geq 1$. □

Lecture 24 Eisenstein Extensions

24.1 Proof continued

We finish off the proof started last time.

Proof continued. Now write

$$f(x) = \prod_{i=1}^{n}(x - \alpha_i)$$

where by α_i we mean the Galois conjugates of $\alpha = \alpha_1$. Thus

$$|f(\beta_0)| = \prod_{i=1}^{n}|\beta_0 - \alpha_i| < |\sigma(\alpha) - \alpha|^n$$

for all $\sigma(\alpha) \neq \alpha$. Take j such that

$$|\beta_0 - \alpha_j| = \min_i |\beta_0 - \alpha_i|,$$

whence

$$|\beta_0 - \alpha_j| < |\sigma(\alpha) - \alpha|$$

for all $\sigma(\alpha) \neq \alpha$.

Since f is irreducible, there exists σ_j such that $\sigma_j(\alpha_j) = \alpha$. Set $\beta = \sigma_j(\beta_0)$. Then

$$|\beta - \alpha| = |\sigma_j(\beta - \alpha)| = |\beta_0 - \alpha_j| < |\sigma(\alpha) - \alpha|$$

for all $\sigma(\alpha) \neq \alpha$, meaning that β belongs to α.

Hence by Krasner's lemma $K(\alpha) \subset K(\beta)$, and since

$$\begin{array}{c} K(\beta) \\ | \\ K(\alpha) \\ | \\ K \end{array}$$

with $[K(\alpha) : K] = \deg f = n$, we have moreover $[K(\beta) : K] \leq \deg g = n$, so $K(\alpha) = K(\beta)$ and hence $g(x)$ is irreducible. □

Corollary 24.1.1. *Take the same assumptions as in the previous proposition. Then every root of $g(x)$ belongs to exactly one root of $f(x)$, so in particular the roots of $g(x)$ yield the same extensions as the roots of $f(x)$.*

Proof. Let α be a root of $f(x)$. By Proposition 23.2.3, there exists a root of $g(x)$, say β, that belongs to α. Let $\beta_1 = \beta, \beta_2, \ldots, \beta_n$ be the roots of $g(x)$.

Since $g(x)$ is irreducible, there exists $\sigma_i \in \mathrm{Gal}(K^{sep}/K)$ such that $\sigma_i(\beta) = \beta_i$. Then β_i belongs to $\sigma_i(\alpha)$, which is a root of $f(x)$.

Date: April 5th, 2018.

Suppose β is a root of $g(x)$ belonging to two roots of $f(x)$, say α and $\sigma(\alpha)$ with $\sigma(\alpha) \neq \alpha$. Then $|\alpha - \beta| < |\sigma(\alpha) - \alpha|$ by definition, and since Galois conjugates don't affect valuations, we can apply σ^{-1} to the right-hand side, so

$$|\sigma(\alpha) - \beta| < |\sigma^{-1}(\sigma(\alpha)) - \sigma(\alpha)| = |\sigma(\alpha) - \alpha|$$

since $\sigma^{-1}(\sigma(\alpha)) = \alpha \neq \sigma(\alpha)$.

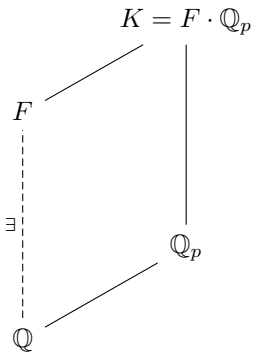
Hence

$$|\sigma(\alpha) - \alpha| = |(\sigma(\alpha) - \beta) - (\beta - \alpha)| < |\sigma(\alpha) - \alpha|,$$

a contradiciton. So roots of $f(x)$ and $g(x)$ are in one-to-one correspondence. □

Corollary 24.1.2. *Let K be a finite extension of $\mathbb{Q}_p$. Then there exists a finite extension F of $\mathbb{Q}$ contained in K such that $K = F \cdot \mathbb{Q}_p$.*

Proof. We are considering the situation



Suppose $K = \mathbb{Q}_p(\alpha)$ (this is possible since the field has characteristic 0 and is separable, meaning that it must be a simple extension). Let $f(x) \in \mathbb{Q}_p[x]$ be the monic minimal polynomial α over $\mathbb{Q}_p$. Now take $g(x) \in \mathbb{Q}[x]$ such that $\|f - g\| < C(f)$, so $g(x)$ is irreducible and has a root β such that $\mathbb{Q}_p(\beta) = \mathbb{Q}_p(\alpha) = K$, since β belongs to α.

Set $F = \mathbb{Q}(\beta)$, then $F\mathbb{Q}_p = \mathbb{Q}_p(\beta) = K$. □

24.2 Eisenstein Extension

The basis of this discussion is a generalisation of Eisenstein's criterion for irreducible polynomials.

Proposition 24.2.1 (Eisenstein's criterion)**.** *Suppose A is a commutative ring with unity. Let $f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n \in A[x]$. Suppose there exists a prime ideal $\mathcal{P} \subset A$ such that $a_0 \notin \mathcal{P}$, $A_i \in \mathcal{P}$ for all $i = 1, 2, \ldots, n$, and $a_n \notin \mathcal{P}^2$. Then $f(x)$ is irreducible.*

Moreover, if $f(x)$ is monic and A is integrally closed, then $(f(x))$ is a prime ideal in $A[x]$.

Compare this to the classical Eisenstein criterion over $\mathbb{Q}$, where instead of a prime ideal $\mathcal{P}$ we have a prime number $p \in \mathbb{Z}$.

In the discussion that follows, let K be a field complete with respect to a non-archimedean valuation $|\cdot|$. Let $\mathcal{O}_K$ be the valuation ring and $\mathcal{M}_K$ be the maximal ideal.

Definition 24.2.2 (Eisenstein polynomial)**.** Let $f(x) = x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n \in \mathcal{O}_K[x]$. If $|a_i| < 1$ (i.e. $a_i \in \mathcal{M}_K$) for all $i = 1, 2, \ldots, n$, and $a_n \notin \mathcal{M}_K^2$, then $f(x)$ is called an ***Eisenstein polynomial***.

Remark 24.2.3. Note that Eisenstein polynomials are necessarily irreducible since they satisfy Eiseinstein's criterion.

Moreover, if $|\cdot|$ is not discrete (meaning that we aren't a discrete valuation ring and hence might not have a unique maximal ideal), then there are no Eisenstein polynomials since $\mathcal{M}_K = \mathcal{M}_K^2$.

For $\alpha \in \mathcal{M}_K$, $|\alpha| < 1$, and since the valuation isn't discrete there exists $\{ \alpha_n \} \subset \mathcal{M}_K$ such that $|\alpha_n| \to 1$. Hence $|\alpha_n| > |\alpha|$ for $n > M$ large enough.

Thus $|\alpha/\alpha_n| < 1$, but $\alpha = \alpha_n \cdot \alpha/\alpha_n$ is a product of two elements in $\mathcal{M}_K$, so $\alpha \in \mathcal{M}_K^2$ as well.

Definition 24.2.4. An extension L of K is ***Eisenstein*** if $L = K(\alpha)$ when α is a root of an Eisenstein polynomial.

Lemma 24.2.5. *Let K be a local field. Then there are only finitely many Eisenstein extensions of K of fixed degree prime to* $\mathrm{char}(K)$.

Proof. Let

$$X = \mathcal{M}_K \times \mathcal{M}_K \times \ldots \times \mathcal{M}_K \times (\mathcal{M}_K \setminus \mathcal{M}_K^2)$$

be the space of coefficients of Eisenstein polynomials of degree n, where we have n sets multiplied together above.

If $\boldsymbol{a} = (a_1, a_2, \ldots, a_n) \in X$, then

$$f_{\boldsymbol{a}}(x) = x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n \in \mathcal{O}_K[x]$$

is an Eisenstein polynomial and hence irreducible. Crucially, every Eisenstein extension of K of degree n arises from adjoining a root of some $f_{\boldsymbol{a}}(x)$ for $\boldsymbol{a} \in X$, since they give us all Eisenstein polynomials.

Since $\gcd(\mathrm{char}(K), n) = 1$, $f'_{\boldsymbol{a}}(x) \neq 0$, since the leading coefficient of the formal derivative is n. Hence $f_{\boldsymbol{a}}(x)$ is separable, and thus Proposition 23.2.3 applies since we are deaing with a finite separable extension.

Now for each $\boldsymbol{a} \in X$ there exists a neighbourhood $U_{\boldsymbol{a}} \subset X$ of $\boldsymbol{a}$ such that if $\boldsymbol{b} \in U_{\boldsymbol{a}}$, then the rotos of $f_{\boldsymbol{a}}(x)$ and $f_{\boldsymbol{b}}(x)$ yield the same extensions of K since their roots belong to each other.

Now $\mathcal{M}_K$ is compact (since K is local) and hence

$$\mathcal{M}_K^2 = (\pi^2) = \{ x \mid |x| \leq |\pi|^2 \} = \{ x \mid |x| < |\pi| \}$$

is both closed and open. Hence $\mathcal{M}_K \setminus \mathcal{M}_K^2$ is closed in $\mathcal{M}_K$ and therefore compact.

Thus X is the product of compact sets and hence is compact in the product topology, so there exists $\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_m \in X$ such that

$$X = \bigcup_{i=1}^{m} U_{\boldsymbol{a}_i}.$$

Therefore every Eisenstein extension of K of degree n is of the form $K(\alpha)$ with α a root of $f_{\boldsymbol{a}_i}(x)$ for $i = 1, 2, \ldots, m$. Hence there are only finitely many Eisenstein extensions of K of degree n. □

Lemma 24.2.6. *Let K be a field complete with respect to a discrete non-archimedean valuation $|\cdot|$. Suppose L is a separable Eisenstein extension of K. Then we have*

(*i*) *L is totally ramified over K, i.e. $\mathcal{M}_K = (\pi_K)$ is totally ramified on $\mathcal{O}_L$.*

(*ii*) *If $L = K(\alpha)$ with α a root of an Eisenstein polynomial over K, then α is a uniformiser of L, i.e. $\mathcal{M}_L = (\pi_L) = (\alpha)$, so $\alpha = \pi_L \cdot u$ with $u \in \mathcal{O}_L^\times$.*

(*iii*) *If π_L is any uniformiser of L, then $\mathcal{O}_L = \mathcal{O}_K[\pi_L]$.*

Lecture 25 Totally Ramified Extensions

25.1 Proof of Lemma

Proof. Suppose

$$f(x) = x^n + a_1 x^{n-1} + \ldots + a_{n-1}x + a_n \in \mathcal{O}_K[x]$$

is Eisenstein and separable. Let $\alpha = \alpha_1, \alpha_2, \ldots \alpha_n$ be the roots of $f(x)$. Then $L = K(\alpha)$. By Corollary 23.1.4, $|\alpha_i| = |\alpha_j|$ for every i and j, with $|\cdot|$ being the extension of the valuation on K to K^{sep}. Let $\mathcal{M}_K = (\pi_K)$.

Since

$$f(x) = \prod_{i=1}^{n}(x - \alpha_i),$$

we must have

$$a_n = (-1)^n \prod_{i=1}^{n} \alpha_i,$$

and since $f(x)$ is Eisenstein $a_n \in \mathcal{M}_k \setminus \mathcal{M}_K^2$, implying $|a_n| = |\pi_K|$. Hence $|\alpha_i|^n = |\pi_K|$ for all i, and so $|\alpha| = |\pi_K|^{1/n}$¿

Let π_L be a uniformiser of $\mathcal{O}_L$, i.e. $\mathcal{M}_L = (\pi_L)$, and write $\pi_K = \pi_L^e \cdot u$ with $u \in \mathcal{O}_L^\times$ and $e = e(\mathcal{M}_L/\mathcal{M}_K)$ and $\alpha = \pi_L^r \cdot v$ with $v \in \mathcal{O}_L^\times$. Then

$$|\pi_K|^{1/n} = |\alpha| = |\pi_L|^r = (|\pi_K|^{1/e})^r = |\pi_K|^{r/e},$$

implying $1/n = r/e$, i.e. $e = n \cdot r$. But we also have $n = e \cdot f$, so $r = 1$ and $e = n$, so L is a totally ramified extension of K, and α is a uniformiser of $\mathcal{O}_L$ since $r = 1$.

For the third and final part we want to prove $\mathcal{O}_L = \mathcal{O}_K[\pi_L]$. Since L is a totally ramified extension of K, the inertial degree $f(\mathcal{M}_L/\mathcal{M}_K) = 1$, so

$$\frac{\mathcal{O}_K}{\mathcal{M}_K} \cong \frac{\mathcal{O}_L}{\mathcal{M}_L}$$

implying $\mathcal{O}_L = \mathcal{O}_K + \pi_L\mathcal{O}_= \mathcal{O}_K[\pi_L] + \pi_L\mathcal{O}_L$.

For $\alpha \in \mathcal{O}_L$, write $\alpha = \alpha_1 + \beta_1$ with $\alpha_1 \in \mathcal{O}_K[\pi_L]$ and $\beta_1 \in \pi_L\mathcal{O}_L$, then write $\beta_1 = \pi_L(\alpha_2 + \beta_2)$ with $\alpha_2 \in \mathcal{O}_K[\pi_L]$ and $\beta_2 \in \pi_L\mathcal{O}_L$, and so forth.

Hence in the end

$$\alpha = \alpha_1 + \pi_L\alpha_2 + \pi_L^2\alpha_3 + \ldots + \pi_L^{r-1}\alpha_r + \pi_L^r\beta_r,$$

Date: April 10th, 2018.

so $\mathcal{O}_L = \mathcal{O}_K[\pi_L] + \pi_L^k \mathcal{O}_L$ for all $k \in \mathbb{N}$.

Now note that $\{ 1, \pi_L, \pi_L^2, \ldots, \pi_L^{n-1} \}$ is an integral basis for L over K, with $n = [L : K]$. Hence

$$\mathcal{O}_K \ni \Delta = \operatorname{disc}(1, \pi_L, \ldots, \pi_L^{n-1}) = \pi_K^m \cdot u = \pi_L^{mn} \cdot v$$

with $u \in \mathcal{O}_K^\times$ and $v \in \mathcal{O}_L^\times$.

Note that $\Delta \mathcal{O}_L \subset \mathcal{O}_K[\pi_L]$ (the proof of this is the same as that for the ring of integers being a finite rank $\mathbb{Z}$-module). Take π_k with $k \geq mn$. We then have $\pi_L^k \mathcal{O}_L \subset \Delta \mathcal{O}_L \subset \mathcal{O}_K[\pi_L]$, so for k large enough $\pi_L^k \subset \mathcal{O}_K[\pi_L]$, so the last β_r term above goes away. □

Lemma 25.1.1. *Let K be a field complete with respect to a discrete, non-archimedean valuation $|\cdot|$. Then a finite separable extension L of K is totally ramified if and only of L is an Eisenstein extension of K.*

Proof. The reverse direction is the last Lemma. For the forward direction, suppose L is a totally ramified extension of K, and let $n = [L : K]$. Let π_L be a uniformiser of L.

We claim $L = K(\pi_L)$. To see this, let $E = K(\pi_L)$. Then $\pi_K \mathcal{O}_L = \pi_L^n \mathcal{O}_L$ since L is a totally ramified extension of K, and therefore

$$|\pi_K|^{1/n} = |\pi_L| \geq |\pi_K|^{1/[E:K]}$$

since $[E : K] \leq n$ and $|\pi_K| < 1$. Also

$$e(\mathcal{M}_E / \mathcal{M}_K) = e = e(\mathcal{M}_L / \mathcal{M}_K) = n$$

since

$$|\pi_L| = |\pi_K|^{\operatorname{ord}_{\mathcal{M}_E}(\pi_L)/e(\mathcal{M}_E/\mathcal{M}_K)},$$

with $\operatorname{ord}_{\mathcal{M}_E}(\pi_L) = 1$ since $\pi_L \mathcal{O}_E = \mathcal{M}_E$. Now $e(\mathcal{M}_E/\mathcal{M}_K) \leq [E : K]$, so $[E : K] = n$, implying $L = K(\pi_L)$.

Now let $f(x) = x^n + a_1 x^{n-1} + \ldots + a_{n-1} x + a_n \in \mathcal{O}_K[x]$ be the monic minimal polynomial of π_L over K. Let $\pi_L = \pi_1, \pi_2, \ldots, \pi_n$ be the roots of $f(x)$. Then $|\pi_i| = |\pi_j| < 1$ for all i and j, an $|a_i| < 1$ by the strong triangle inequality since a_i are polynomials in π_j. Moreover since

$$a_n = (-1)^n \prod_{i=1}^{n} \pi_i$$

we have $|a_n| = |\pi_L|^n = |\pi_K|$, implying $a_n = \pi_K \cdot u$ for some $u \in \mathcal{O}_K^\times$, and $a_n \in \mathcal{M}_K \setminus \mathcal{M}_K^2$, so $f(x)$ is an Eisenstein polynomial, meaning that $L = K(\pi_L)$ is an Eistenstein extension of K. □

Corollary 25.1.2. *Let K be a local field. Then there exists only finitely many extensions of K of a fixed degree prime to* $\operatorname{char}(K)$ *that are totally ramified.*

Proof. By Lemma 25.1.1 totally ramified extensions are the same as Eisenstein extensions, and by Lemma 24.2.5 there are only finitely many Eisenstein extensions of a fixed degree prime to $\operatorname{char}(K)$. □

25.2 Unramified Extensions

Let K be a local field with L a finite separable extension of K. Then L is an unramified extension of K if and only if $e(L/K) = e(\mathcal{M}_L/\mathcal{M}_K) = 1$ if and only if $\mathcal{M}_K\mathcal{O}_L = \mathcal{M}_L$ if and only if π_K is a uniformiser of K implies π_K is a uniformiser of L¿

Proposition 25.2.1. *Let K be a local field with residue field $k = \mathcal{O}_K/\mathcal{M}_K$. Then there exists a bijection between the set of finite separable unramified extensions L of K and finite extensions ℓ of k, sending L to ℓ, the residue field of L, satisfying*

(*i*) *if $K' \leftrightarrow k'$ and $K'' \leftrightarrow k''$, then $K' \subset K''$ if and only if $k' \subset k''$;*

(*ii*) $\mathrm{Gal}(L/K) \cong \mathrm{Gal}(\ell/k)$ *with the isomorphism given by $\sigma \mapsto \sigma|_{\mathcal{O}_L} = \overline{\sigma}$ which sends $\mathcal{M}_L \mapsto \mathcal{M}_L$ (in general it must send maximal ideal to maximal ideal, but there is only one here). So it induces $\overline{\sigma}$ on $\mathcal{O}_L/\mathcal{M}_L$ which fixes $\mathcal{O}_K/\mathcal{M}_K$.*

Before we prove this, note that L being a finite, separable, unramified extension of K implies that L is a Galois extension of K, whence $\mathrm{Gal}(L/K)$ in the theorem is well-defined.

To see this, take $\alpha \in \mathcal{O}_L$ and let $f(x)$ be the monic minimal polynomial of α over K, so $f(x) \in \mathcal{O}_K[x]$ is irreducible, reducing to $\overline{f}(x) \in \mathcal{O}_K/\mathcal{M}_K[x] = k[x]$.

Now $\deg \overline{f} \leq \deg f$, and in particular since f is monic they are equal, and $\overline{\alpha}$ being the reduction of α modulo $\mathcal{M}_K$ is a root of $\overline{f}(x)$.

Then $\overline{f}(x)$ splits in $\ell[x]$ since its a finte extension of a finite field, so it is Galois, and hence $f(x)$ splits in $L[x]$ by Hensel's lemma, so L is a Galois extension of K.

Lecture 26 Unramified Extensions

26.1 Classifying Unramified Extensions

Proof of Proposition 25.2.1. Let $p = \mathrm{char}(k)$.

Step one: Suppose $\gcd(p, m) = 1$. The irreducible factors of $x^m - 1$ in $k[x]$ are the irreducible factors of $x^m - 1$ in $\mathcal{O}_K[x]$ modulo $\mathcal{M}_K$. That is,

$$x^m - 1 = f_1(x)^{e_1} f_2(x)^{e_2} \cdot \ldots \cdot f_r(x)^{e_r} \in k[x]$$

with f_i irreducible in $k[x]$ and

$$x^m - 1 = g_1(x)^{n_1} g_2(x)^{n_2} \cdot \ldots \cdot g_r(x)^{n_r} \in \mathcal{O}_K[x]$$

with g_i irreducible in $\mathcal{O}_K[x]$, then for each f_i there exists a g_i such that $f_i \equiv g_i \pmod{\mathcal{M}_K}$ and $\deg f_i = \deg g_i$.

To prove this it suffices to show the reduction of an irreducible factor $g(x)$ of $x^m - 1$ in $\mathcal{O}_K[x]$ remains irreducible in $k[x]$.

Let $g(x) \equiv \overline{g}(x) \pmod{\mathcal{M}_K}$ in $k[x]$. We want to show that $\overline{g}(x)$ is irreducible in $k[x]$ and $\deg \overline{g} = \deg g$.

Date: April 12th, 2018.

Note that $g(x) \mid x^m - 1$ in $\mathcal{O}_K[x]$ implies $\overline{g}(x) \mid x^m - 1$ in $k[x]$, and the latter is separable in $k[x]$ since $\gcd(p, m) = 1$ implies its derivative $mx^{m-1} \neq 0$. Hence $\overline{g}(x)$ is separable.

Let $f_0(x) \in k[x]$ be a monic irreducible factor of $\overline{g}(x)$. Let $f(x) \in \mathcal{O}_K[x]$ be a monic lift of $f_0(x)$, i.e. $f(x) \equiv f_0(x) \pmod{\mathcal{M}_K}$. Since the lift is monic we have $\deg f = \deg f_0$.

Let α be any root of $f(x)$ and let $L = K(\alpha)$. Then

$$[L : K] = \deg f(x) = \deg f_0(x) \leq \deg \overline{g}(x) \leq \deg g(x).$$

Moreover $\overline{g}(x) \equiv g(x) \pmod{\mathcal{M}_K}$, and $f(\alpha) = 0$ implying $\overline{f}(\overline{\alpha}) = f_0(\overline{\alpha}) = 0$, hence $\overline{g}(\overline{\alpha}) = 0$. Hence $\overline{g}$ has a root $\overline{\alpha} \equiv \alpha \pmod{\mathcal{M}_K}$.

Now $g'(\alpha) \equiv \overline{g}'(\overline{\alpha}) \not\equiv 0 \pmod{\mathcal{M}_K}$ since $\overline{g}$ is separable, and so by Hensel's lemma $g(x)$ has a zero, say β, in $\mathcal{O}_K$, and $L \supset K(\beta)$. Moreover

$$\deg g(x) \geq [L : K] \geq [K(\beta) : K] = \deg g(x)$$

since g is irreducible, and hence the above degrees are all equal, so $\deg f_0 = \deg \overline{g} = \deg g$, so $\overline{g}$ is also irreducible, as desired.

Step two: Suppose $[\ell : k] = n$. Then there exists a unique unramified extension K_n of K that is finte, separable, and K_n has residue field ℓ.

To prove this, write $\ell = k(\alpha_0)$ for some α_0. Since $\ell^\times$ is a cyclic group of order $|\ell| - 1$, α_0 is a root of $x^m - 1$ in $k[x]$, where $m = |\ell| - 1$, and $\gcd(p, m) = 1$. Let $f_0(x)$ be the monic minimal polynomial of $x^m - 1$. By step one, there exists an irreducible factor $f(x) \in \mathcal{O}_K[x]$ of $x^m - 1$ such that $f(x) \equiv f_0(x) \pmod{\mathcal{M}_K}$ and $\deg f = \deg f_0$.

Let α be any root of $f(x)$ and put $K_n = K(\alpha)$. Then $[K_n : K] = \deg f = \deg f_0 = [\ell : k] = n$, and remark that

$$ef = n \geq f(K_n/K) = \dim_k \frac{\mathcal{O}_{K_n}}{\mathcal{M}_{K_n}}.$$

Let $\overline{\alpha} \equiv \alpha \pmod{\mathcal{M}_K}$. Then for $f_0(\overline{\alpha}) \equiv f(\alpha) \pmod{\mathcal{M}_K}$ and $f(\alpha) = 0$. Now $[k(\overline{\alpha}) : k] = \deg f_0 = n$, and

$$\dim_k \frac{\mathcal{O}_{K_n}}{\mathcal{M}_{K_n}} = n$$

implying $\mathcal{O}_{K_n}/\mathcal{M}_{K_n} \cong \ell$, so K_n is an unramified extension of K since $n = ef = f$.

Now on to uniqueness. Suppose L is a finite, separable, unramified extension of K such that the residue field of L is ℓ. Since $f_(x)$ has a root $\overline{\alpha}$ in $\ell = \mathcal{O}_L/\mathcal{M}_L$, we have $f(\overline{\alpha}) \equiv 0 \pmod{\mathcal{M}_L}$. Hensel's lemma thus implies $f(x) \in \mathcal{O}_K[x]$ has a root in $\mathcal{O}_L$, and since K_n is a Galois extension of K we have $K_n \subset L$, because it means $K_n = K(\alpha)$ must be equal to $K(\alpha_i)$ for the Galois conjugates of α.

Now L is an unramified extension of K, meaning $e = 1$, so $f = [L : K]$ whence

$$[L : K] = [\ell : k] = [K_n : K],$$

implying that $K_n = L$ and moreover $k' \subset k''$ implies $K' \subset K''$ (the opposite inclusion is trivial).

Step three: Let us show that $\mathrm{Gal}(K_n/K) \cong \mathrm{Gal}(\ell/k)$ sending $\sigma \mapsto \overline{\sigma}$.

Note that $|\mathrm{Gal}(K_n/K)| = |\mathrm{Gal}(\ell/k)|$ since their degrees are equal, so it suffices to show that the map between these two is injective. Let $f(x)$ and $f_0(x)$ be as above. By Hensel's lemma, any root of $f_0(x)$ in ℓ lifts to a root of $f(x)$ in $\mathcal{O}_{K_n}$. Let $\alpha_1, \alpha_2, \ldots, \alpha_n$ be the roots of $f(x)$ and $\overline{\alpha}_1, \overline{\alpha}_2, \ldots, \overline{\alpha}_n$ be the roots of $f_0(x)$ such that $\overline{\alpha}_i \equiv \alpha_i \pmod{\mathcal{M}_K}$.

Suppose $\sigma \in \mathrm{Gal}(K_n/K)$ such that $\sigma \neq \mathrm{Id}$. Then there exists i and j such that $\sigma(\alpha_i) = \alpha_j$ with $i \neq j$, implying $\overline{\sigma}(\overline{\alpha}_i) = \overline{\alpha}_j \neq \overline{\alpha}_i$, so $\overline{\alpha} \neq \mathrm{Id}$ in $\mathrm{Gal}(\ell/k)$. So $\ker(\mathrm{Gal}(K_n/K) \mapsto \mathrm{Gal}(\ell/k)) = \{\mathrm{Id}\}$, so it is injective, and hence $\mathrm{Gal}(K_n/K) \cong \mathrm{Gal}(\ell/k)$. □

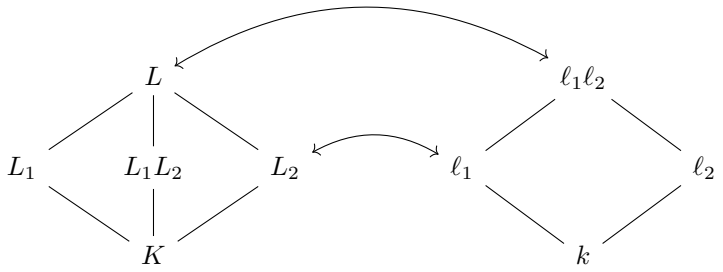
Corollary 26.1.1. *Let K be a local field.*

(*i*) *The composition of two finite, separable, unramified extensions of K is unramified.*

(*ii*) *If L is any separable, algebraic extension of K (possibly of infinite degree), then there exists a unique maximal unramified subextension $K \subset L_{ur} \subset L$.*

(*iii*) *Given any integer n, there exists a unique unramified extension K_n of K of degree n. Moreover $\mathrm{Gal}(K_n/K) \cong \mathbb{Z}/n\mathbb{Z} = \mathrm{Gal}(\ell/k)$.*

Proof. We have the following situation



Some of this needs to be proven. First, $\ell_1\ell_2$ is a finite extension of k, so by the previous proposition $\ell_1\ell_2/k$ is in one to one correspondence with some L/K. Now $\ell_1 \subset \ell_1\ell_2$ implies $L_1 \subset L$, and similarly $\ell_2 \subset \ell_1\ell_2$ implies $L_2 \subset L$¡ so $L_1L_2 \subset L$.

Also L is an unramified extension of K, so L_1L_2 is as well, because ramification index is multiplicative, so

$$1 = e(L/K) = e(L/L_1L_2)e(L_1L_2/K).$$

For the second property, take

$$L_{ur} = \prod_i E_i$$

where E_i are finite, separable, unramified extensions of K.

The third property we proved in the course of the last proof. □

Corollary 26.1.2. *Let K be a local field. Then there exists finitely many extensions of K of fixed degree with ramification index that is prime to* $\mathrm{char}(K)$.

Proof. Suppose L is such an extension of K of degree n. Then we have $[L_{ur} : K] \mid n$ and by the previous corollary, for each $d \mid n$ there exists a unique unramified extension K_d of K. So L_{ur} is in the set of K_d for $d \mid n$, and that's a finite set. Moreover $[L : L_{ur}] = e(L/K)$ which is coprime to $\mathrm{char}(K)$, and by Corollary 25.1.2 there are only finitely many totally ramified extensions L of L_{ur} with $\gcd([L : L_{ur}], p) = 1$ for every L_{ur}. Hence there are finitely many L of the sort desired. □

Example 26.1.3. There are only finitely many quadratic extensions of $\mathbb{Q}_p$ (note that $\mathrm{char}(\mathbb{Q}_p) = 0$, so the coprimality condition holds automatically). Moreiver we have either $e = 1$ and $f = 2$, for unramified extensions, or $e = 2$ and $f = 1$, for totally ramified ones.

Compare this to quadratic extensions $\mathbb{Q}(\sqrt{D})$ of $\mathbb{Q}$; here there are infinitely many. ▲

Lecture 27 Unramified Extensions

27.1 Tamely and Wildly Ramified Extensions

Let K be a local field with residue field $k = \mathcal{O}_K/\mathcal{M}_K$ and let $p = \mathrm{char}(k)$. Let L be a finite, separable extension of K, and let π_K be a uniformiser of K.

Definition 27.1.1. (*i*) L is an ***unramified*** extension of K if $e(L/K) = 1$, meaning that prime ideals in K remain prime in L.

(*ii*) L is a ***tamely ramified*** extension of K if $e(L/K) \neq 1$ and $p \nmid e(L/K)$.

(*iii*) L is a ***wildly ramified*** extension of K if $p \mid e(L/K)$.

What we want to get at with this is the following:

$$\begin{array}{c} L \\ \Big| {\scriptstyle p^r} \\ L_t \\ \Big| {\scriptstyle \text{tamely ramified}} \\ L_{ur} \\ \Big| {\scriptstyle \text{unramified}} \\ K \end{array}$$

Lemma 27.1.2. *Suppose L is a totally ramified extension of K. Suppose there exists $\beta_0 \in L^\times$ such that $|\beta_0|^e = |\pi_K|$ for some e, $p \nmid e$. Then there exists $\beta \in L$ and a uniformiser α of K such that $\beta^e = \alpha$.*

Proof. Write $\beta_0^e = \pi_K \cdot u$ with $u \in \mathcal{O}_K^\times$. Since L is a totally ramified extension of K, $f(L/K) = 1$, i.e.

$$\frac{\mathcal{O}_L}{\mathcal{M}_K} \cong \frac{\mathcal{O}_K}{\mathcal{M}_K}$$

Date: April 17th, 2018.

so there exists some $u_0 \in \mathcal{O}_K$ such that $u \pmod{\mathcal{M}_L} = u_0 \pmod{\mathcal{M}_K}$. Put $\alpha = \pi_K \cdot u_0 \in \mathcal{O}_K$.

Note that

$$|\beta_0^e - \alpha| = |\pi_K \cdot u - \pi_K \cdot u_0| = |\pi_K(u - u_0)| < |\pi_K| = |\alpha|$$

since $u - u_0 \in \mathcal{O}_K$, making its valuation bounded by 1. Let $\beta_1, \beta_2, \ldots, \beta_e$ be the roots of

$$f(x) = x^e - \alpha = \prod_{i=1}^{e}(x - \beta_i).$$

Hence

$$|\alpha| > |\beta_0^e - \alpha| = |f(\beta_0)| = \prod_{i=1}^{e}|\beta_0 - \beta_i|,$$

so there exists some i_0 such that $|\beta_0 - \beta_{i_0}| < |\alpha|^{1/e} = |\beta_{i_0}|$ since $f(\beta_{i_0}) = 0$ if and only if $\beta_{i_0}^e - \alpha = 0$.

We now claim that $K(\beta_{i_0}) \subset K(\beta_0) \subset L$ (letting $\beta = \beta_{i_0}$).

To prove this, note that $p \nmid e$ means that $e \in \mathcal{M}_K$, so $|e| = 1$. Hence

$$|\beta_{i_0}|^{e-1} = |e||\beta_{i_0}|^{e-1} = |f'(\beta_{i_0})| = \prod_{\substack{j=1 \\ j \neq i_0}}^{e} |\beta_{i_0} - \beta_j|.$$

Since

$$|\beta_{i_0} - \beta_j| \leq \max\{\, |\beta_{i_0}|, |\beta_j| \,\} = |\beta_{i_0}|$$

for every j we have

$$|\beta_{i_0}|^{e-1} = \prod_{\substack{j=1 \\ j \neq i_0}}^{e} |\beta_{i_0} - \beta_j| \leq |\beta_{i_0}|^{e-1},$$

so $|\beta_{i_0} - \beta_j| = |\beta_{i_0}|$ for all j. This means that $|\beta_0 - \beta_{i_0}| < |\beta_{i_0} - \beta_j|$ for all $j \neq i_0$, so by Krasner's lemma $K(\beta_{i_0}) \subset K(\beta_0) \subset L$ whence $\beta_{i_0} \in L$. □

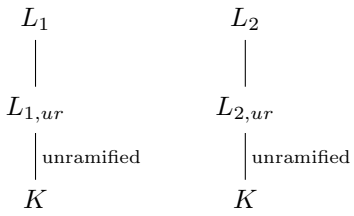
Corollary 27.1.3. *(i) L is a totally tamely ramified extension of K if and only if there exist uniformisers π_K of K and π_L of L such that $\pi_L^n = \pi_K$ where $n = [L : K]$ and $\mathrm{char}(k) = p \nmid n$.*

(ii) If L_1 and L_2 are both tamely ramified extensions of K, then so is L_1L_2.

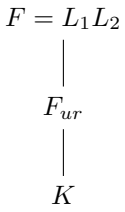
Proof. (i) For the reverse direction, consider $f(x) = x^n - \pi_K$. This is irreducible by Eisenstein's criterion and has a root π_L with $L = K(\pi_L)$. This is totally ramified since it's Eisenstein, and $e(L/K) = n$, and $p \nmid n$ by assumption.

For the forward direction, suppose L is totally tamely ramified over K. Then $\pi_K'\mathcal{O}_L = \pi_L'^e\mathcal{O}_K$ with $e = [L : K] = n$ and $p \nmid e$. Then by Lemma 27.1.2 there exists a π_K in K and π_L in L such that $\pi_L^e = \pi_L^n = \pi_K$. Since $|\pi_L|^e = |\pi_K|$, π_L is a uniformiser of L.

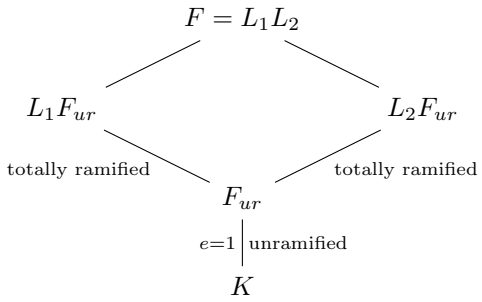
(*ii*) First we reduce to the case where L_1 and L_2 are not only tamely ramified, but totally tamely ramified. To see this, we have



and consider



Then

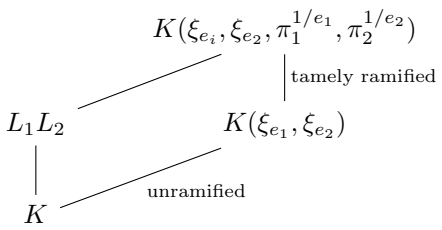


Call $L_1' = L_1F_{ur}$, $L_2' = L_2F_{ur}$, so $F = L_1L_2 = L_1'L_2'$, and treat F_{ur} as K'. Then F is tamely ramified over K', so likewise over K since ramification indices are multiplicative.

Hence assume L_1 and L_2 are totally ramified over K. By (*i*), there exist uniformisers $\pi_{L_1} \in L_1$ and $\pi_{L_2} \in L_2$ and $\pi_1, \pi_2 \in K$ such that $\pi_{L_1}^{[L_1:K]} = \pi_1$ and $\pi_{L_2}^{[L_2:K]} = \pi_2$. Then $L_i = K(\pi_{L_i}) = K(\pi_i^{1/e_i}) \subset K(\xi_{e_i}, \pi_i^{1/e_i})$, and $e_i = [L_i : K]$ since the extensions are totally ramified.

Now $p \nmid e_i$ means that $K(\xi_{e_i})/K$ is unramified (cf. the proof of $\mathbb{Q}(\xi_{e_i})/Q$ of same). Hence $K(\xi_{e_i}, \pi_i^{1/e_i})/K(\xi_{e_i})$ is totally tamely ramified since $x^{e_i} - \pi_i$ is Eisenstein and $p \nmid e_i$.

The situation then is



where L_1L_2 is a tamely ramified extension of K since its ramification index divides that of the labelled tamely ramified extension above. □

Proposition 27.1.4. *Let L be a finte, separable extension of a local field K. Then there exist unique subfields $K \subset L_{ur} \subset L_t \subset L$ such that*

(*i*) *L_{ur} is an unramified extension of K,*

(*ii*) *L_t is a totally tamely ramified extension of K, and*

(*iii*) *L is a degree p^r extension of L_t for some r, where $p = \mathrm{char}(k)$ and L is a totally ramified extension of L_t.*

Proof. We've done (*i*) before. For (*ii*),

$$L_t = \prod_i E_i$$

for every $L_{ur} \subset E_i \subset L$ being tamely ramified.

For (*iii*), write $[L : L_t] = p^r e'$ with $p \nmid e'$. Let π_L be a uniformiser in L, and π_t a uniformiser in L_t. Since L is totally ramified over L, $\pi_t \mathcal{O}_L = \pi_L^{p^r e'} \mathcal{O}_L$, so $|\pi_L^{p^r}|^{e'} = |\pi_t|$, $p \nmid e'$. By Lemma 27.1.2 there exists $\beta \in L$ and $\pi' \in L_t$, uniformisers, such that $\beta^{e'} = \pi'$. (Note that β might not be a uniformiser since $e' \neq [L_t : L]$.)

Now β is a root of $f(x) = x^{e_1} - \pi' \in \mathcal{O}_{L_t}[x]$, which is Eisenstein, so

$$\begin{array}{c} L \\ \Big| p^r \\ L_t(\beta) \\ \Big| e' \\ L_t \\ \Big| \\ L_{ur} \end{array}$$

where $L_t(\beta)$ is tamely ramified over L_{ur}. But L_t is the maximal tamely ramified extension of L_{ur}, so $L_t = L_t(\beta)$, i.e. $e' = 1$. □

27.2 Decomposition Group and Intertia Group

Let L and K be number fields with $[L : K] = n$, and assume L is a Galois extension of K. Let $P \subset \mathcal{O}_K$ be a prime ideal and $P\mathcal{O}_L = (Q_1 Q_2 \cdots Q_r)^e$ (the extension being Galois implies that they all have the same ramification index), where $e = e(Q_i/P)$ and $f = f(Q_i/P)$, and $ref = n$.

The Galois group $\mathrm{Gal}(L/K)$ acts transitively on Q_j.

Fix $Q = Q_1$, say. Then for each Q lying above P we define the ***decomposition group***

$$D = D_P = D(Q/P) = \{\, \sigma \in \mathrm{Gal}(L/K) \mid \sigma(Q) = Q \,\}$$

and the ***intertia group***

$$I = I_P = I(Q/P) = \{\, \sigma \in \mathrm{Gal}(L/K) \mid \sigma(\alpha) \equiv \alpha \pmod{Q} \text{ for all } \alpha \in \mathcal{O}_L \,\}.$$

Remark 27.2.1. We clearly have $I \leq D \leq \mathrm{Gal}(L/K)$ are subgroups, and for $\sigma \in D$ we have

$$\begin{array}{ccc} \mathcal{O}_L & \xrightarrow{\sigma} & \mathcal{O}_L \\ \big| & & \big| \\ \mathcal{O}_L/Q & \xrightarrow{\bar{\sigma}} & \mathcal{O}_L/Q \end{array}$$

so σ induces $\bar{\sigma}$ where $\bar{\sigma} \in \mathrm{Gal}(\ell/k)$, with $\ell = \mathcal{O}_L/Q$ and $k = \mathcal{O}_K/P$.

Lecture 28 Decomposition and Inertia Group

28.1 Decomposition and Inertia

From last time we have the diagram

$$\begin{array}{ccc} \mathcal{O}_L & \xrightarrow{\sigma} & \mathcal{O}_L \\ \big| & & \big| \\ \mathcal{O}_L/Q & \xrightarrow{\bar{\sigma}} & \mathcal{O}_L/Q = \ell \\ \big| & & \big| \\ \mathcal{O}_K/P & \longrightarrow & \mathcal{O}_K/P = k \end{array}$$

This gives us the group homomorphism $\psi\colon D \to \mathrm{Gal}(\ell/k)$ by $\sigma \mapsto \bar{\sigma}$, which has $\ker\psi = I$ since I by definition are those elements of $\mathrm{Gal}(L/K)$ that act as the identity modulo Q on $\mathcal{O}_L$.

This in fact gives rise to the short exact sequence

$$1 \longrightarrow I \longrightarrow D \xrightarrow{\psi} \mathrm{Gal}(\ell/k) \longrightarrow 1.$$

The last step in the sequence, the surjectivity of ψ, is nontrivial, and we shall endeavour to prove it in a moment.

In the discussion that follows we will, for a subgrou $H \leq G = \mathrm{Gal}(L/K)$, refer to

$$L_H = \{\, x \in L \mid \sigma(x) = x \text{ for all } \sigma \in H \,\}$$

as the ***fixed field*** of H.

Definition 28.1.1. The field L_D is the ***decomposition field*** and L_I is the ***inertia field***. Set $Q_D = Q \cap L_D$ and $Q_I = Q \cap L_I$.

Theorem 28.1.2. *With the notation and conditions as above, we have*

			ramification index	*inertial degree*
$\{1\}$	L	Q		
$\vert\wedge$	$\vert e$	$\vert$	e	1
I	L_I	Q_I		
$\vert\wedge$	$\vert f$	$\vert$	1	f
D	L_D	Q_D		
$\vert\wedge$	$\vert r$	$\vert$	1	1
G	K	P		

Date: April 19th, 2018.

Proof. We'll prove these indices and degrees one at a time.

Step one: $[L_D : K] = r$.

By Galois theory, $[L_D : K] = [G : D]$. Let G/D denote the set of left cosets of D (D might not be a normal subgroup, so this might not be a proper quotient group) and define $\varphi\colon G/D \to \{ Q_1 = Q, Q_2, \dots, Q_r \}$, the image being the set of primes lying above P, by $\varphi(\sigma D) = \sigma(Q)$.

This is well-defined because if $\sigma_1 D = \sigma_2 D$, then $\sigma_1(Q) = \sigma_2(\psi(Q))$, but ψ fixes Q, and moreover it's surjective since G acts transitively on primes above P.

We claim that φ is also injective: if $\varphi(\sigma D) = \varphi(\tau D)$, then $\sigma(Q) = \tau(Q)$, so $\tau^{-1}\sigma \in D$, so $\sigma D = \tau D$. Hence φ is bijective, and so $|G/D| = r$.

Step two: $e(Q_D/P) = 1$ and $f(Q_D/P) = 1$. By step one, $[L_D : K] = r$, and this implies $[L : L_D] = ef$ since $[L : K] = erf$.

Now $D = \mathrm{Gal}(L/L_D)$ acts transitively on primes in L lying above Q_D, but D fixes Q, so Q is the only prime lying above Q_D, so $r(Q/Q_D) = 1$.

Hence

$$ef = [L : L_D] = e(Q/Q_D)f(Q/Q_D)$$

where the first factor is bounded by e and the second bounded by f since ramification indices and intertial degrees are multiplicative. Hence we must have $e(Q/Q_D) = e$ and $f(Q/Q_D) = f$, so $e(Q_D/P) = f(Q_D/P) = 1$.

Step three: $f(Q/Q_I) = 1$ and therefore $f(Q_I/Q_D) = f$ (since their product is f).

To see this, note that $f(Q/Q_I) = 1$ if and only if $\ell = \mathcal{O}_L/Q \cong \mathcal{O}_{L_I}/Q_I = k_I$, so it suffices to show $\mathrm{Gal}(\ell/k_I) = \{ \mathrm{Id} \}$.

For any $\theta \in \ell$, let $\alpha \in \mathcal{O}_L$ correspond to θ, so $\alpha \pmod{Q} = \theta$. Then

$$g(x) = \prod_{\sigma \in \mathrm{Gal}(L/L_I)} (x - \sigma(\alpha)) \in \mathcal{O}_{L_I}[x].$$

Modulo Q this is $\bar{g}(x) \in k_I[x]$. Since $\sigma(\alpha) \equiv \alpha \pmod{Q}$, $\bar{g}(x) = (x - \theta)^m$, with $m = |\mathrm{Gal}(L/L_I)|$. Hence the only Galois conjugate of θ is θ itself, so for $\tau \in \mathrm{Gal}(\ell/k_I)$, $\tau(\theta) = \theta$ for all $\theta \in \ell$, so $\theta = \mathrm{Id}$.

Step four: $[L_I : L_D] = f$ and hence $e(Q_I/Q_D) = 1$, $e(Q/Q_I) = e$, and $[L : L_I] = e$.

Now $\psi\colon D \to \mathrm{Gal}(\ell/k)$ by $\sigma \mapsto \bar{\sigma}$ has $\ker \psi = I$. We don't know they if this is surjective, so all we know so far is

$$|D/I| \leq |\mathrm{Gal}(\ell/k)| = [\ell : k] = f,$$

the last equality by definition. On the other hand,

$$|D/I| = [L_I : L_D] \geq e(Q_I/Q_D)f(Q_I/Q_D),$$

but $f(Q_I/Q_D) = f$ from above, so $[L_I : L_D] = f$, whence $e(Q_I/Q_D) = 1$. □

By the sizes of the sets in the very last step we then finally confirm

Corollary 28.1.3. *We have the following short exact sequence*

$$1 \longrightarrow I \longrightarrow D \xrightarrow{\psi} \mathrm{Gal}(\ell/k) \longrightarrow 1$$

since ψ is surjective.

Corollary 28.1.4. *Suppose D is a normal subgroup of G. Then P splits into r distinct primes in L_D.*

If I is also normal in G, then each prime $Q'_P \subset \mathcal{O}_{L_D}$ lying above P remains prime in L_I and $Q'_D\mathcal{O}_L = Q_L^e$ in $\mathcal{O}_L$.

Proof. For the first claim, simply note

$$P\mathcal{O}_{L_D} = (Q_1 Q_2 \cdots Q'_r)^{e'},$$

where by the above results $e' = e$ and $r' = r$.

For the second part, L_I is a Galois extension of L since I is normal in G, and hence L_I is a Galois extension of L_D as well. Hence

$$f = r(Q'_I/Q'_D)e(Q'_I/Q'_D)f(Q'_I/Q'_D)$$

where $r(Q'_I/Q'_D)$ is the number of primes lying above Q'_D in $\mathcal{O}_{L_I}$. But we know that $e(Q'_I/Q'_D) = 1$ and $f(Q'_I/Q'_D) = f$, so the number of primes above Q'_D must be exactly 1, whence $Q'_D\mathcal{O}_{L_I} = Q'_I$ in $\mathcal{O}_{L_I}$ and $Q'_D\mathcal{O}_L = Q'_I\mathcal{O}_L = Q_L^e$ in $\mathcal{O}_L$. □

These decomposition and inertia fields are special, as we will discuss in what follows. Let K' be an intermediate field, i.e. $K' = L_H$ for some $H \leq G$, and

$$\begin{array}{ccc} \{1\} & L & Q \\ |\wedge & | & | \\ H & K' & P' \\ |\wedge & | & | \\ G & K & P \end{array}$$

With this setup,

Theorem 28.1.5. *(i) L_D is the largest intermediate field K', $K \subset K' \subset L$, such that $e(P'/P) = f(P'/P) = 1$.*

(ii) L_D is the smallest K' such that Q is the only prime in $\mathcal{O}_L$ lying above P'.

(iii) L_I is the largest K' such that $e(P'/P) = 1$.

(iv) L_I is the smallest K' such that Q is totally ramified over P', in other words $e(Q/P') = [L : K']$.

Definition 28.1.6. Let F and K be number fields, with F an extension of K, and let $P \subset \mathcal{O}_K$ be a prime ideal. We say that P ***splits completely*** in F is P splits into $[F : K]$ distinct primes, i.e. $e(Q/P) = f(Q/P) = 1$ for all $Q \subset \mathcal{O}_F$ lying above P.

Corollary 28.1.7. *Assume $D = D(Q/P)$ is normal in $\mathrm{Gal}(L/K)$. Then P splits completely in K', $K \subset K' \subset L$, if and only if $K' \subset L_D$.*

Proof. The forward direction is immediate by the maximality of L_D in the theorem above.

For the reverse direction, D is normal in G means that L_D is a Galois extension over K, and so P splits completely in L_D and $K \subset K' \subset L_D$. So $e(Q_D/P) = f(Q_D/P) = 1$, and we know that each of those can be written as $e(Q_D/P')e(P'/P)$ and $f(Q_D/P')f(P'/P)$ respectively, since they are multiplicative, and they too must then be 1. □

Lecture 29 More on Ramification of Extensions

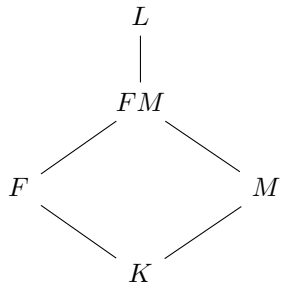
29.1 Splitting of Primes

Theorem 29.1.1. *Let K be a number field. Let F and M be two finite extensions of K. Fix a prime P in K.*

(*i*) *If P is unramified in both F and M, then P is unramified in FM.*

(*ii*) *If P splits completely in both F and M, then P splits completely in FM.*

Proof. (*i*) Let L be anuy normal extension of K such that $FM \subset L$. In other words we have the situation



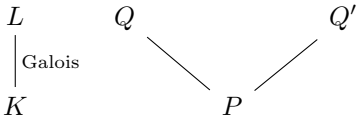
Let P' be any prime in FM lying above P, and let Q_F and Q_M be primes above P in F and M, respectively. By assumption $e(Q_F/P) = 1$.

Now let $I = I(Q/P)$ for some Q in L lying over P. Since P is unramified in F, $F \in L_I$, the largest fiend with P unramified. Similarl $M \in L_I$, so $FM \subset L_I$, so P is unramified in FM.

(*ii*) Having $e(Q_F/P) = f(Q_F/P) = q$ implies $F \in L_D$, and likewise $M \subset L_D$, so $FM \subset L_D$, whence $e(P'/P) = f(P'/P) = q$, meaning that P splits completely in FM. □

Corollary 29.1.2. *Let L/K be number fields. Let P be a prime in K. Then P is unramified (respectively splits completely) in L if and only if P is unramified (respectively splits completely) in the normal closure M of L.*

Suppose we have a Galois extension L of K, with two different primes Q and Q' lying above a prime P in K. In other words,



Date: April 24th, 2018.

Then in other words $P\mathcal{O}_L = QQ' \cdots$, and since the Galois group acts transitively on these, there exists some $\sigma \in \mathrm{Gal}(L/K)$ such that $\sigma(Q) = Q'$. The decomposition and intertia groups are also related; namely $D(Q'/P) = \sigma D(Q/P)\sigma^{-1}$ and $I(Q'/P) = \sigma I(Q/P)\sigma^{-1}$.

In particular, if $\mathrm{Gal}(L/K)$ is abelian, then $D(Q/P)$ and $I(Q/P)$ depend only on P, not Q.

Recall that

$$1 \longrightarrow I(Q/P) \longrightarrow D(Q/P) \longrightarrow \mathrm{Gal}(\ell/k) \longrightarrow 1$$

is a short exact sequence.

Since the Galois group above is the Galois group of finite fields it is cyclic, and it is generated by the Frobenius automorphism.

Let $\mathbb{F}_{p^f}$ be a finite field of order p^f and let $\mathbb{F}$ be a finite field extension of $\mathbb{F}_{p^f}$ of degree n. Then

$$\mathrm{Gal}(\mathbb{F}/\mathbb{F}_{p^f}) = \langle \tau \rangle$$

where $\tau(x) = x^{p^f}$ is the ***Frobenius automorphism***.

Let L/K be number fields. Assume L is a Galois extension of K, and let P be a prime in K and Q a prime in L lying above P. Assume P is unramified in L. Then $L_I = L$, so $I = \mathrm{Gal}(L/L_I) = \{ 1 \}$ is trivial.

So we have an isomorphism $\psi\colon D(Q/P) \to \mathrm{Gal}(\ell/k)$, $\sigma \mapsto \bar{\sigma}$, and in particular $\phi \mapsto \bar{\phi}$, where $\bar{\phi} = x^{\mathrm{N}(P)}$, $\mathrm{N}(P) = [\mathcal{O}_K : P]$. Thus $D(Q/P) = \langle \phi \rangle$, and $\phi(\alpha) \equiv \alpha^{\mathrm{N}(P)} \pmod{Q}$ for all $\alpha \in \mathcal{O}_L$.

Remark 29.1.3. The above ϕ is the only element in $D(Q/P)$ with this property. Correspondingly, we call $\phi = \phi(Q \mid P)$ the ***Frobenius automorphism*** of Q over P.

This has the special property that

$$\phi(\sigma(Q \mid P) = \sigma\phi(Q \mid P)\sigma^{-1}$$

for all $\sigma \in \mathrm{Gal}(L/K)$.

Remark 29.1.4. The conjugacy class of $\phi(Q \mid P)$ in $\mathrm{Gal}(L/K)$ is uniquely determined by the unramified prime in P.

In particular, if $G = \mathrm{Gal}(L/K)$ is abelian, then $\phi(Q \mid P)$ is uniquely determined by P. We have $\phi = \phi(Q \mid P)$ for all primes Q lying over P, and $\phi(\alpha) \equiv \alpha^{\mathrm{N}(P)} \pmod{Q}$ for all Q lying above P.

Thus $\phi(\alpha) \equiv \alpha^{\mathrm{N}(P)} \pmod{P\mathcal{O}_L}$, with $P\mathcal{O}_L = Q_1Q_2 \cdots$ being the product of all primes above P.

Theorem 29.1.5. *Let L and K be number fields with L a Galois extension of K. Let P be a prime in K that is unramified in L. Then for each prime Q in L lying above P, there is a unique $\phi \in \mathrm{Gal}(L/K)$ such that $\phi(\alpha) \equiv \alpha^{\mathrm{N}(P)} \pmod{Q}$ for every $\alpha \in \mathcal{O}_L$.*

Moreover if $\mathrm{Gal}(L/K)$ is abelian, then ϕ depends only on P and $\phi(\alpha) \equiv \alpha^{\mathrm{N}(P)} \pmod{P\mathcal{O}_L}$ for all $\alpha \in \mathcal{O}_L$.

Exercise 29.1.6. Let L and K be number fields, with L being a Galois extension of K. Let P be a prime in K unramified in L. Then P splits completely in L if and only if $\phi(Q \mid P) = \mathrm{Id}$ for all Q in L above P.

Theorem 29.1.7. *Let K be a number field. Let $p \in \mathbb{Z}$ be a prime. Then p is ramified in K if and only if $p \mid \operatorname{disc}(K)$.*

Proof. We've done the forward direction a long time ago. For the opposite direction, assume $p \mid \operatorname{disc}(K)$. Fir an integral basis $\alpha_1, \alpha_2, \ldots, \alpha_n$ for $\mathcal{O}_K$. Then $\operatorname{disc}(K) = \det(\operatorname{Tr}(\alpha_i\alpha_j))$, and consider all integers modulo p.

We have $\det(\operatorname{Tr}(\alpha_i\alpha_j)) = 0$ in $\mathbb{F}_p$ since $p \mid \operatorname{disc}(K)$, so the row vectors

$$v_i = (\operatorname{Tr}(\alpha_i\alpha_1), \operatorname{Tr}(\alpha_i\alpha_2), \ldots, \operatorname{Tr}(\alpha_i\alpha_n))$$

for $i = 1, 2, \ldots, n$ are linearly dependent over $\mathbb{F}_p$. Hence there exists some $m_i \in \mathbb{Z}$, not all $m_i \equiv 0 \pmod{p}$, such that

$$m_1v_1 + m_2v_2 + \ldots + m_nv_n \equiv 0 \pmod{p}.$$

The jth coordinate of this is

$$\sum_{i=1}^{n} m_i \operatorname{Tr}(\alpha_i\alpha_n) = \operatorname{Tr}\left(\Big(\sum_{i=1}^{n} m_i\alpha_i\Big)\alpha_j\right) \equiv 0 \pmod{p}$$

for every $j = 1, 2, \ldots, n$, since trace is linear. Set

$$\alpha = \sum_{i=1}^{n} m_i\alpha_i,$$

then $\operatorname{Tr}(\alpha\alpha_j) \equiv 0 \pmod{p}$ for all j, and since α_j form an integral basis for $\mathcal{O}_K$ this is true for all of $\mathcal{O}_K$, whence $\operatorname{Tr}(\alpha\mathcal{O}_K) \subset p\mathbb{Z}$.

Note that $\alpha \notin P\mathcal{O}_K$ since not all $m_i \equiv 0 \pmod{p}$. Now assume p is unramified in K.

Then $p\mathcal{O}_K = Q_1Q_2\cdots Q_r$, with Q_i all distinct primes in K. Thus $\alpha \notin Q_i$ for some i, say, $\alpha \notin Q_1 = Q$, and let L be the normal closure of K over $\mathbb{Q}$. Hence P is unramified in L by the previous corollary.

Let Q_L be any prime in L lying above Q. Since $\alpha \notin Q$, we also have $\alpha \notin Q_L$ (else $\alpha \in Q_L \cap K = Q$).

We claim $\operatorname{Tr}_{L/\mathbb{Q}}(\alpha\mathcal{O}_L) \subset p\mathbb{Z}$.

To prove this, note that

$$\operatorname{Tr}_{L/\mathbb{Q}}(\alpha\mathcal{O}_L) = \operatorname{Tr}_{K/\mathbb{Q}}(\operatorname{Tr}_{L/K}(\alpha\mathcal{O}_L)) \subset \operatorname{Tr}_{K/\mathbb{Q}}(\alpha\mathcal{O}_K) \subset p\mathbb{Z},$$

since $\operatorname{Tr}_{L/K}(\alpha\mathcal{O}_L) = \alpha \operatorname{Tr}_{L/K}(\mathcal{O}_L) \subset K$. Now fix any $\beta \in Q_i$, $i = 2, 3, \ldots, r$, with $\beta \notin Q = Q_1$. (Such a β exists by the Chinese remainder theorem since Q_i are coprime.)

We make two claims: For each $\gamma \in \mathcal{O}_L$, we have

(*i*) $\operatorname{Tr}_{L/\mathbb{Q}}(\alpha\beta\gamma) \in Q$,

(*ii*) $\sigma(\alpha\beta\gamma) \in Q$ for each $\sigma \in \operatorname{Gal}(L/\mathbb{Q}) = G$, $\sigma \notin D = D(Q/P)$.

(*i*) Since $\operatorname{Tr}_{L/\mathbb{Q}}(\alpha\mathcal{O}_L) \subset p\mathbb{Z} \subset Q$, we also have $\operatorname{Tr}_{L/\mathbb{Q}}(\alpha\beta\gamma) \in Q$ since $\beta\gamma \in \mathcal{O}_L$.

(*ii*) For $\sigma \in G \setminus D$, $\sigma^{-1}(Q) \neq Q$. Thus $\beta \in \sigma^{-1}(Q)$, whence $\sigma(\beta) \in Q$. Hence $\sigma(\alpha\beta\gamma) \in Q$ since $\sigma(\alpha\gamma)\sigma(\beta) \in Q$ since Q is prime.

From the claim, therefore,

$$\sum_{\sigma\in D}\sigma(\alpha\beta\gamma) = \mathrm{Tr}_{L/\mathbb{Q}}(\alpha\beta\gamma) - \sum_{\sigma\in G\setminus D}\sigma(\alpha\beta\gamma).$$

If we modulo this by Q,

$$\sum_{\sigma\in D}\bar{\sigma}(\bar{\alpha}\bar{\beta}\bar{\gamma}) \equiv 0$$

in $\mathcal{O}_L/Q$ for every $\bar{\gamma}\in\mathcal{O}_L/Q$.

Now $\bar{\alpha}\bar{\beta}\neq 0$ in $\mathcal{O}_L/Q$ since $\alpha,\beta\notin Q$, so

$$\sum_{\sigma\in D}\bar{\sigma}(x) = 0$$

for every $x\in\mathcal{O}_L/Q$, whence

$$\sum_{\sigma\in D}\bar{\sigma} \equiv 0$$

as a function. Recall that $D\cong\mathrm{Gal}(\ell/k)$ since p is unramified.

This is a contradiction since distinct Galois objects are linearly independent, so p is ramified. □

Lecture 30 The Different Ideal

30.1 Duals

Example 30.1.1. Let $K=\mathbb{Q}(\alpha)$ with $\alpha^3-\alpha-1=0$. Then $\mathcal{O}_K=\mathbb{Z}[\alpha]$. We have $\mathrm{disc}(K)=-23$, so $p=23$ is the only prime ramified in K.

Now $23\mathcal{O}_K = PQ^2$, where $P=(23,\alpha-3)$ and $Q=(23,\alpha-10)$. Hence $e(Q/p)=2>1$, and $e(P/p)=1$.

We want to detect that Q is the prime with $e>1$, in general. ▲

Definition 30.1.2. Let K be a number field of degree n. Then L is called a ***lattice*** in K if L is of the form

$$L = \mathbb{Z}\alpha_1+\mathbb{Z}\alpha_2+\ldots+\mathbb{Z}\alpha_n$$

where $\{\alpha_1,\alpha_2,\ldots,\alpha_n\}$ is a basis for K over $\mathbb{Q}$.

Consider the bilinear form $K\times K\to\mathbb{C}$ defined by $(x,y)\mapsto\mathrm{Tr}_{K/\mathbb{Q}}(xy)$. This is called the ***trace product***, and is an analogue of the inner product in $\mathbb{R}^n$.

Definition 30.1.3. Let L be a lattice in K. The ***dual lattice*** of L is defined as

$$L^\vee = \{\,\alpha\in K \mid \mathrm{Tr}_{K/\mathbb{Q}}(\alpha L)\subset\mathbb{Z}\,\}.$$

Theorem 30.1.4. *Let K be a number field. Let $L\subset K$ be a lattice with $\mathbb{Z}$-basis $\alpha_1,\alpha_2,\ldots,\alpha_n$. Then*

$$L^\vee = \mathbb{Z}\alpha_1^\vee+\mathbb{Z}\alpha_2^\vee+\ldots+\mathbb{Z}\alpha_n^\vee,$$

Date: April 26th, 2018.

where $\{ \alpha_i^\vee \}$ *is the dual basis of* $\{ \alpha_i \}$ *with respect to the trace product (and is indeed also a basis for* K *over* $\mathbb{Q}$*). In particular,* $L^\vee$ *is a lattice.*

Here $\alpha_i^\vee$ *is defined by*

$$\operatorname{Tr}_{K/\mathbb{Q}}(\alpha_i^\vee \alpha_j) = \delta_{ij} = \begin{cases} 1, & \text{if } i = j \\ 0, & \text{if } i \neq j. \end{cases}$$

Theorem 30.1.5. *Let* $K = \mathbb{Q}(\alpha)$ *and let* $f(x) \in \mathbb{Q}[x]$ *be the minimal polynomial of* α *over* $\mathbb{Q}$*. Write*

$$f(x) = (x - \alpha)(c_{n-1}(\alpha)x^{n-1} + \ldots + c_1(\alpha)x + c_0(\alpha))$$

with $c_i(\alpha) \in K$*. Then the dual basis to* $\{ 1, \alpha, \alpha^2, \ldots, \alpha^{n-1} \}$ *with respect to the trace product is*

$$\left\{ \frac{c_0(\alpha)}{f'(\alpha)}, \frac{c_1(\alpha)}{f'(\alpha)}, \ldots, \frac{c_{n-1}(\alpha)}{f'(\alpha)} \right\}.$$

In particular, if $K = \mathbb{Q}(\alpha)$ *with* $\alpha \in \mathcal{O}_K$*, then*

$$\begin{aligned} \mathbb{Z}[\alpha]^\vee &= (\mathbb{Z} \cdot 1 + \mathbb{Z}\alpha + \ldots + \mathbb{Z}\alpha^{n-1})^\vee \\ &= \frac{1}{f'(\alpha)}(\mathbb{Z} \cdot 1 + \mathbb{Z}\alpha + \ldots + \mathbb{Z}\alpha^{n-1}) = \frac{1}{f'(\alpha)}\mathbb{Z}[\alpha]. \end{aligned}$$

Note that this does *not* say $c_i(\alpha) = 1$, but there exists a transformation of basis that makes it so.

Theorem 30.1.6. *For any fractional ideal* I *in* K*,* $I^\vee$ *is also a fractional ideal and* $I^\vee = I^{-1}\mathcal{O}_K^\vee$*.*

Theorem 30.1.7. *The dual lattice* $\mathcal{O}_K^\vee$ *is the largest fractional ideal in* K *whose elements all have trace in* $\mathbb{Z}$*.*

Remark 30.1.8. The theorem does not say $\mathcal{O}_K^\vee$ is the set of all elements in K with integral trace. In fact,

$$\{ \alpha \in K \mid \operatorname{Tr}_{K/\mathbb{Q}}(\alpha) \in \mathbb{Z} \}$$

is an additive group, but it is not a fractional ideal.

Example 30.1.9. Take $K = \mathbb{Q}(\sqrt{-1})$. Then $\mathcal{O}_K = \mathbb{Z}[\sqrt{-1}]$ and

$$\mathcal{O}_K^\vee = \frac{1}{2}\mathbb{Z}[\sqrt{-1}],$$

but

$$\{ \alpha \in K \mid \operatorname{Tr}_{K/\mathbb{Q}}(\alpha) \in \mathbb{Z} \} = \frac{1}{2}\mathbb{Z} + \mathbb{Q}\sqrt{-1}$$

is not a fractional ideal. ▲

Definition 30.1.10. The ***different ideal*** D_K of K is

$$D_K = (\mathcal{O}_K^\vee)^{-1} = \{ x \in K \mid x\mathcal{O}_K^\vee \subset \mathcal{O}_K \},$$

so $D_K^{-1} = \mathcal{O}_K^\vee$.

Remark 30.1.11. Since $\mathcal{O}_K \subset \mathcal{O}_K^\vee$, $(\mathcal{O}_K^\vee)^{-1} \subset \mathcal{O}_K^{-1} = \mathcal{O}_K$, i.e. $D_K \subset \mathcal{O}_K$. In other words D_K is an integral ideal.

Theorem 30.1.12. *Let K be a number field. Then* $\mathrm{N}(D_K) = [\mathcal{O}_K : D_K] = |\mathrm{disc}(K)|$.

Theorem 30.1.13. *The prime factors of D_K are the primes in K that ramify over $\mathbb{Q}$.*

More precisely, for any prime ideal $P \subset \mathbb{Q}$ lying above $p \in \mathbb{Z}$ with $e(P/p\mathbb{Z}) = e$, if

$$D_K = P^s Q$$

with $\gcd(P, Q) = 1$, *then*

$$\begin{cases} s = e - 1 & \text{if } p \nmid e \\ s \geq e & \text{if } p \mid e. \end{cases}$$

So if $e(P/p\mathbb{Z}) = 1$, i.e. P is unramified, then P is not in D_K.

Example 30.1.14. Let $K = \mathbb{Q}(\sqrt{D})$ with D square free. Then

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}[\sqrt{D}], & \text{if } D \not\equiv 1 \pmod 4 \\ \mathbb{Z}[\frac{1+\sqrt{D}}{2}] & \text{if } D \equiv 1 \pmod 4, \end{cases}$$

and

$$\mathrm{disc}(K) = \begin{cases} 4D, & \text{if } D \not\equiv 1 \pmod 4 \\ D & \text{if } D \equiv 1 \pmod 4. \end{cases}$$

Two cases: if $D \not\equiv 1 \pmod 4$, the minimal polynomial of $\sqrt{D}$ over $\mathbb{Q}$ is $f(x) = x^2 - D$. We have $f'(\sqrt{D}) = 2\sqrt{D}$, so

$$\mathcal{O}_K^\vee = frac1f'(\sqrt{D})\mathbb{Z}[\sqrt{D}],$$

so $D_K = (\mathcal{O}_K^\vee)^{-1} = (2\sqrt{D})\mathcal{O}_K$.

In the second case, $D \equiv 1 \pmod 4$. Let $\alpha = 1 + \sqrt{D}/2$. We have $f(x) = x^2 - x + (1 - D)/4$, and $f'(\alpha) = \sqrt{D}$, so $D_K = \sqrt{D}\mathcal{O}_K$.

Hence

$$D_K = \begin{cases} 2\sqrt{D} & \text{if } D \not\equiv 1 \pmod 4 \\ \sqrt{D} & \text{if } D \equiv 1 \pmod 4. \end{cases}$$

and

$$\mathrm{N}(D_K) = \begin{cases} 4|D|, & \text{if } D \not\equiv 1 \pmod 4 \\ |D| & \text{if } D \equiv 1 \pmod 4. \end{cases} = |\mathrm{disc}(K)|. \qquad \blacktriangle$$

Index