ALGEBRAIC NUMBER THEORY
NOTES

CHARLOTTE CHAN

Contents

1. Unique Prime Factorization of Ideals: 21 September 2010

This corresponds somewhat to Chapter 1, §3 of J. Neukirch's Algebraic Number Theory text. We begin with a definition.

Definition 1.1. A ring R is called *Noetherian* if every ideal $\mathfrak{a} \lhd R$ is finitely generated.

We state a theorem.

Theorem 1.1. *If K is an algebraic number field and $\mathcal{O}_K$ its ring of integers, then $\mathcal{O}_K$ is Noetherian, integrally closed, and every nonzero prime ideal of $\mathcal{O}_K$ is maximal.*

Proof. It is trivial that $\mathcal{O}_K$ is integrally closed. Consider the ideal $\mathfrak{a} \lhd \mathcal{O}_K$ and choose $0 \neq \alpha \in \mathfrak{a}$. Then $\alpha\mathcal{O}_K \subseteq \mathfrak{a} \subseteq \mathcal{O}_K$. Now, $\mathcal{O}_K$ is a free $\mathbb{Z}$-module of rank n, where $n = [K : \mathbb{Q}]$, and $\alpha\mathcal{O}_K$ is also a free $\mathbb{Z}$-module of rank n, so $\mathfrak{a}$ must also be a free $\mathbb{Z}$-module of rank n. From this, the fact that $\mathfrak{a}$ is finitely generated as an ideal of $\mathcal{O}_K$ comes for free, and since $\mathfrak{a}$ was an arbitrarily chosen ideal, we can conclude that $\mathcal{O}_K$ is Noetherian.

We now have left to prove that every nonzero prime ideal is maximal. Now, $\mathfrak{p} \lhd R$, $\mathfrak{p}$ a prime ideal $\Leftrightarrow R/\mathfrak{p}$ is an integral domain. Since $\mathfrak{p} \lhd R$ is maximal, then $R/\mathfrak{p}$ is an integral domain $\Leftrightarrow$ $R/\mathfrak{p}$ is a field. (In general, every maximal ideal is prime.) Hence it is sufficient to show that if $\mathfrak{p}$ is a nonzero prime ideal of $\mathcal{O}_K$, then $\mathcal{O}_K/\mathfrak{p}$ is a field.

Let $\mathfrak{p} \lhd \mathcal{O}_K$ be a nonzero prime ideal. Consider $\mathfrak{p} \cap \mathbb{Z}$. Now, $\mathfrak{p} \cap \mathbb{Z}$ is the nonzero prime ideal (p) in $\mathbb{Z}$, for p a rational prime: Take $0 \neq y \in \mathfrak{p}$. y is integral over $\mathbb{Z}$ so it satisfies $y^n + a_1y^{n-1} + a_2y^{n-2} + \cdots + a_{n-1}y + a_n = 0$ for some $a_1, \ldots, a_n \in \mathbb{Z}$. Since we assume $a_n \neq 0$ and each term $a_{n-i}y^i$, $i = 1, \ldots, n-1$ is an element of $\mathfrak{p}$, then we must have that $a_n \in \mathfrak{p}$ so $a_n \in \mathfrak{p} \cap \mathbb{Z} = (p)$, which proves that (p) is nonzero. It is clear that (p) is a prime ideal.

Now let us consider the quotient ring $\mathcal{O}_K/\mathfrak{p}$. We want to prove that $\mathcal{O}_K/\mathfrak{p}$ is finite. We know already that $\mathcal{O}_K = \mathbb{Z}\alpha_1 + \ldots \mathbb{Z}\alpha_n$, $\alpha_1, \ldots, \alpha_n \in \mathcal{O}_K$, so each α_i is integral over $\mathbb{Z}$. Since $\mathcal{O}_K$ is generated over $\mathbb{Z}/\mathfrak{p} \cap \mathbb{Z} = \mathbb{Z}/p\mathbb{Z}$ by the image of $\alpha_1, \ldots, \alpha_k$ under the map $\mathcal{O}_K \to \mathcal{O}_K/\mathfrak{p}$, then $\mathcal{O}_K/\mathfrak{p}$ must be finite. (Another way to see this is the following. We know already that any $x \in \mathcal{O}_K$ can be written in the form $n_1\alpha_1 + \cdots + n_k\alpha_k$ where each $n_i \in \mathbb{Z}$. So if we have $x = n_1\alpha_1 + \cdots + n_k\alpha_k, y = m_1\alpha_1 + \cdots + m_k\alpha_k$ and $n_i \equiv m_i \pmod{p}$ for all i, then certainly $x - y \in \mathfrak{p}$, which would mean that x, y are equivalent in $\mathcal{O}_K$. This means that $|\mathcal{O}_K/\mathfrak{p}| \leq p^n$.) Since $\mathcal{O}_K/\mathfrak{p}$ is a finite ring without zero divisors (we have no zero divisors since $\mathfrak{p}$ is prime, then it follows that $\mathcal{O}_K/\mathfrak{p}$ must necessarily be a field. □

Definition 1.2. A Noetherian, integrally closed integral domain in which every nonzero prime ideal is maximal is called a *Dedekind domain.*

The above definition gives us the liberty of stating Theorem 1.1 in a cleaner way: If K is an algebraic number field and $\mathcal{O}_K$, then $\mathcal{O}_K$ is a Dedekind domain.

It turns out that if we have a Dedekind domain R, then we can generalize the notions of divisibility, lcm, and gcd that we have in $\mathbb{Z}$.

Definition 1.3. Let $\mathfrak{a}, \mathfrak{b} \lhd R$. Then: We say $\mathfrak{a} \,|\, \mathfrak{b}$ if $\mathfrak{b} \subseteq \mathfrak{a}$. The greatest common divisor is $\mathfrak{a} + \mathfrak{b} = \{\alpha + \beta : \alpha \in \mathfrak{a}, \beta \in \mathfrak{b}\}$. The least common multiple is $\mathfrak{a} \cap \mathfrak{b}$. And we define $\mathfrak{ab} = \{\sum_i \alpha_i\beta_i : \alpha_i \in \mathfrak{a}, \beta_i \in \mathfrak{b}\}$, the set of finite sums of products of elements in $\mathfrak{a}, \mathfrak{b}$.

This next important is an amazing thing, and it generalizes the notion of unique prime factorization to principal ideal domains! The connection to Dedekind domains here is that a a Dedekind domain has unique prime factorization if and only if it is a PID.

Theorem 1.2. *Every (nontrivial) ideal $\mathfrak{a} \lhd R$ (i.e. $\mathfrak{a} \neq (0), (1)$) has a factorization $\mathfrak{a} = \mathfrak{p}_1 \ldots \mathfrak{p}_n$ where $\mathfrak{p}_i$ are nonzero prime ideals, unique up to order of factors.*

We will prove two lemmas, after which the theorem will be easy to prove.

Lemma 1.1. *For every nonzero ideal $\mathfrak{a} \lhd R$ there exist nonzero prime ideals satisfying $\mathfrak{p}_1 \ldots \mathfrak{p}_r \subseteq \mathfrak{a}$.*

Proof. We take a maximal counterexample $\mathfrak{a}$. Since $\mathfrak{a}$ is not a prime ideal, we can find $b_1, b_2 \notin \mathfrak{a}$ such that $b_1 b_2 \in \mathfrak{a}$. Let $\mathfrak{a}_1 = (b_1) + \mathfrak{a}, \mathfrak{a}_2 = (b_2) + \mathfrak{a}$. Since $\mathfrak{a}$ was a maximal counterexample, $\mathfrak{a} \subsetneq \mathfrak{a}_1, \mathfrak{a} \subsetneq \mathfrak{a}_2$, and there are nonzero prime ideals such that $\mathfrak{p}_1 \cdots \mathfrak{p}_r \subseteq \mathfrak{a}_1, \mathfrak{q}_1 \cdots \mathfrak{q}_r \subseteq \mathfrak{a}_2$. But then we have $\mathfrak{p}_1 \cdots \mathfrak{p}_r \mathfrak{q}_1 \cdots \mathfrak{q}_s \subseteq \mathfrak{a}_1 \mathfrak{a}_2 \subseteq \mathfrak{a}$, a contradiction. □

Lemma 1.2. *Let $\mathfrak{p}$ be a nonzero prime ideal and define $\mathfrak{p}^{-1} = \{x \in K : x\mathfrak{p} \subseteq R\}$. Then for every nonzero ideal $\mathfrak{a} \lhd R$, we have $\mathfrak{p}^{-1} \supsetneq \mathfrak{a}$.*

Proof. We first prove the special case that $\mathfrak{p}^{-1} \supsetneq R$. It is clear that $\mathfrak{p}^{-1} \subseteq R$, so we have left to show that they are not equal. Let $\mathfrak{p}$ be a nonzero prime ideal and take some nonzero $\alpha \in \mathfrak{p}$. Let r be minimal such that $\mathfrak{p}_1 \cdots \mathfrak{p}_r \subseteq (\alpha) \subseteq \mathfrak{p}$, where each $\mathfrak{p}_i$ is a nonzero prime ideal. (We know we can do this by Lemma 1.1.) Now, some $\mathfrak{p}_i$ must be contained in $\mathfrak{p}$ since otherwise, we would have $b_1 \in \mathfrak{p}_1 \backslash \mathfrak{p}, \ldots, b_n \in \mathfrak{p}_n \backslash \mathfrak{p}$ such that $b_1 \cdots b_r \in \mathfrak{p}$, which can't happen since $\mathfrak{p}$ is prime. So say $\mathfrak{p}_1 \subseteq \mathfrak{p}$. Since R is a Dedekind domain, then $\mathfrak{p}_1$ is maximal, so $\mathfrak{p}_1 = \mathfrak{p}$. Since $\mathfrak{p}_2 \cdots \mathfrak{p}_r \not\subseteq (\alpha)$, then there is some $\beta \in \mathfrak{p}_2 \cdots \mathfrak{p}_r$ such that $\beta \notin (\alpha) = \alpha R$. We know that $\beta\mathfrak{p} \subseteq (\alpha) = \alpha R$ so $\alpha^{-1}\beta\mathfrak{p} \subseteq R$, and since we had $\beta \notin \alpha R \Rightarrow \alpha^{-1}\beta \notin R$, then we have found an element $\gamma = \alpha^{-1}\beta$ such that $\gamma \in \mathfrak{p}^{-1}, \gamma \notin R$. Hence we have that $\mathfrak{p}^{-1} \supsetneq R$.

For the general case, take an ideal $0 \neq \mathfrak{a} \lhd R$ and assume $\mathfrak{a}\mathfrak{p}^{-1} = \mathfrak{a}$. Take any $x \in \mathfrak{p}^{-1}$ and let $\alpha_1, \ldots, \alpha_n$ be generators of $\mathfrak{a}$. (We can pick generators since R is Noetherian.) So $\mathfrak{a} = (\alpha_1) + \cdots + (\alpha_2)$. Hence for each $x\alpha_i$, we can write $x\alpha_i = \sum_{j=1}^{n} \beta_{ij}\alpha_j$, since $x\alpha_i \in \mathfrak{a}\mathfrak{p}^{-1} = \mathfrak{a}$. In matrix form, these equations can be represented as

$$\begin{pmatrix} x-\beta_{11} & \beta_{12} & \cdots & \beta_{1n} \\ \beta_{21} & x-\beta_{22} & \cdots & \beta_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ \beta_{n1} & \beta_{n2} & \cdots & x-\beta_{nn} \end{pmatrix} \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

If d is the determinant of this matrix, then we have $d\alpha_i = 0$ for all i, which forces $d = 0$ since α_i cannot all be 0. This means that x is integral over R, and so $x \in R$ (since R is a Dedekind domain, so it must be integrally closed). So $\mathfrak{p}^{-1} \subseteq R$, which means that $\mathfrak{p}^{-1} = R$, which contradicts the first part of the proof. Hence we can conclude that $\mathfrak{p}^{-1} \supsetneq \mathfrak{a}$ □

2. Minkowski Theory: 28 September 2010 - 5 October 2010

We begin by discussing lattices and the Minkowski space, denoted $K_{\mathbb{R}}$. The finale of our discussion will be the ability to prove the finiteness of the class number. (For reference, this corresponds to Chapter 1, §4 - §6 of Neukirch's book.)

Say K is a number field and we have $[K : \mathbb{Q}] = n$. Since K is separable, then we have n embeddings $\tau : K \to \mathbb{C}$. (This comes easily from Galois. We can write $K = \mathbb{Q}(\alpha)$ and then every embedding is defined by sending α to a power of itself, and there are n distinct choices here.) We define $K_{\mathbb{C}}$ to be the direct product of the image of K under each embedding; i.e.

$$K_{\mathbb{C}} := \prod_{\tau} \mathbb{C}.$$

We have a map $j : K \to K_{\mathbb{C}}$ defined by $a \mapsto (\tau a)$, where (τa) denotes the n-tuple with τa in each component, for every embedding τ. In terms of notation, we will denote τa as $(ja)_\tau$. The usual inner product definition holds on $K_{\mathbb{C}}$:

$$\langle x, y \rangle = \sum_{\tau} x_\tau \overline{y_\tau}.$$

We can also define a linear involution $F : K_{\mathbb{C}} \to K_{\mathbb{C}}$ on this space, i.e. a linear operator whose inverse is itself. If $z = (z_\tau) \in K_{\mathbb{C}}$, then we define F to be such that for every τ, $(Fx)_\tau = \overline{z_{\overline{\tau}}}$. We can check that this is an involution by checking that $FFz = z$. This is an easy check: $(FFz)_\tau = (F(Fz))_\tau = (\overline{Fz})_{\overline{\tau}} = z_\tau$. We also have that

$$\langle Fx, Fy \rangle = \overline{\langle x, y \rangle}.$$

From this, we can define the *Minkowski space*:

$$K_{\mathbb{R}} = \{x \in K_{\mathbb{C}} : Fz = z\}.$$

The inner product on $K_{\mathbb{R}}$ is inherited from that of $K_{\mathbb{C}}$ and it turns out that $K_{\mathbb{R}}$ is F-invariant since for any $a \in K$, we have $(F(ja))_\tau = \overline{ja}_{\overline{\tau}} = \tau a = (ja)_\tau$, where j is the map $j : K \to K_{\mathbb{R}}$. For a more explicit description of $K_{\mathbb{R}}$, we can define

$$K_{\mathbb{R}} = \{(z_\tau) \in K_{\mathbb{C}} : z_\rho \in \mathbb{R}, z_{\overline{\sigma}} = (\overline{z_\sigma})\},$$

where ρ is a real embedding $K \to \mathbb{R}$, and σ is a complex embedding $K \to \mathbb{C}, K \not\to \mathbb{R}$. $K_{\mathbb{R}}$ is an $\mathbb{R}$-vector space of dimension $n = r + 2s$, where r is the number of real embeddings and s is the number of complex conjugate pairs of embeddings. Also, the previously described map $j : K \to K_{\mathbb{R}}$ is the embedding of K into an n-dimensional Euclidean space. All this is important because it turns out that the image of any nonzero ideal $\mathfrak{a} \lhd \mathcal{O}_K$ will be a complete lattice in $K_{\mathbb{R}}$!

Definition 2.1. Let V be an n-dimensional vector space over $\mathbb{R}$. Then the subgroups $\mathbb{Z}v_1 + \cdots + \mathbb{Z}v_m$ where $v_1, \ldots, v_m \in V$ are linearly independent over $\mathbb{R}$ is called a *lattice*. If $m = n$, then we call this a *complete lattice*.

Definition 2.2. The set $\Phi = \{x_1 v_1 + \cdots + x_m v_m : 0 \leq x_i < 1\}$ is a *fundamental domain*.

Clearly, a lattice is a discrete subgroup.

Definition 2.3. Let $\Gamma \leq V$ be a subgroup. It is called *discrete* if for every $\gamma \in \Gamma$ there is a neighborhood of γ in V such that there are no other points of Γ in this neighborhood.

Theorem 2.1. *If Γ is a subgroup of V, then Γ is a lattice if and only if Γ is a discrete subgroup.*

In order to not lose sight of our first goal, to prove Minkowski's big theorem, we will save the proof of Theorem 2.1 for later. For now, we shall also assume that there is a symmetric, positive-definite bilinear form $\langle\ ,\ \rangle : V \times V \to \mathbb{R}$. From this, we get a notion of volume. As an example, if $e_1, \ldots, e_n$ is an orthonormal basis, then the cube spanned by these elements has volume 1. If

$v_1, \ldots, v_n$ are linearly independent vectors, then the fundamental domain Φ has $\text{vol}(\Phi) = |\det(A)|$, where A is the $n \times n$ matrix satisfying

$$A \begin{pmatrix} e_1 \\ \vdots \\ e_n \end{pmatrix} = \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix}.$$

Definition 2.4. The volume of a lattice Γ is the volume of its fundamental domain Φ; i.e. $\text{vol}(\Gamma) = \text{vol}(\Phi)$.

Now we can state and prove Minkowski's Lattice Point Theorem.

Theorem 2.2. *(Minkowski) Let Γ be a complete lattice in an Euclidean vector space of dimension n. Let $X \subseteq V$ be a subset of V that is centrally symmetric and convex. If vol$(X) > 2^n$ vol(Γ), then X contains a nonzero lattice point (i.e. a nonzero element of Γ.)*

Proof. If $\text{vol}(X) > 2^n \text{vol}(\Gamma)$, then $\text{vol}(\frac{X}{2}) > \text{vol}(\Gamma)$. There must be two distinct elements $x_1, x_2 \in \frac{1}{2}X$ such that $x_1 - x_2 \in \Gamma$. This is true since otherwise, we would have

$$\text{vol}(\Phi) \geq \sum_{\gamma \in \Gamma} \text{vol}(\Phi \cap (\frac{1}{2}X + \gamma)) = \sum_{\gamma \in \Gamma} \text{vol}((\Phi - \gamma) \cap \frac{1}{2}X) = \text{vol}(\frac{1}{2}X),$$

which is a contradiction. Hence we can indeed find $x_1, x_2 \in \frac{1}{2}X$ such that $x_1 - x_2 \in \Gamma$, which means that $x_1 - x_2 \in X$ since $x_1 - x_2 = \frac{1}{2}(2x_1) + \frac{1}{2}(-2x_2) \in X$ by the convexity and centrally symmetric property of X. Therefore we conclude that $x := x_1 - x_2 \in X \cap \Gamma$, and so we have found that $x \in X$ is a nonzero lattice point. □

Now that we have proved Minkowski's Lattice Point Theorem, we will go back to fill in the gaps. We first discuss the aforementioned symmetric, positive-definite bilinear form on $K_{\mathbb{R}}$. There is an isomorphism $f : K_{\mathbb{R}} \to \prod_\tau \mathbb{R}$. Defining $x_\rho = z_\rho, x_\sigma = \text{Re}(z_\sigma), x_{\overline{\sigma}} = \text{Im}(z_\sigma)$, we can define the isomorphism to take $z = (z_\tau) \in K_{\mathbb{C}} \mapsto (x_\tau)$. So if we label the real embeddings ρ and label the complex embeddings σ with their conjugates $\overline{\sigma}$, then the τ coordinate of the image of z is:

$$(f(z))_\tau = \begin{cases} z_\tau & \text{if } \tau = \rho \\ \text{Re}(z_\tau) & \text{if } \tau = \sigma \\ \text{Im}(x_\tau) & \text{if } \tau = \overline{\sigma}. \end{cases}$$

We can define a scalar product on $\prod_\tau \mathbb{R}$ by $\langle x, y \rangle = \sum_\tau a_\tau x_\tau y_\tau$ where $a_\tau = \begin{cases} 1 & \tau \text{ is real} \\ 2 & \tau \text{ is complex.} \end{cases}$

Theorem 2.3. *The inner product on $K_{\mathbb{R}}$ agrees with this inner product by the isomorphism.*

So it turns out that $K_{\mathbb{R}}$ is an n-dimensional $\mathbb{R}$-vector space and we have an inner product that corresponds to the usual Lebesgue measure, differing only by a factor of 2^s, where s is the number of pairs of complex embeddings of K. So how do we use this to compute the volume?

Example. Consider $X := \{x = (x_\tau) : |x_\tau| \leq 1\} \subseteq \prod_\tau \mathbb{R}$. Then $\text{vol}(X) = 2^n \cdot 2^s$. (Notice here that we have the usual Lebesgue measure and then an extra factor of 2^s.)

Now let K be an algebraic number field and take a nonzero ideal $\mathfrak{a} \lhd \mathcal{O}_K$. Then $\mathfrak{a}$ has an integral basis, call it $\alpha_1, \ldots, \alpha_n$. Let $d(\mathfrak{a}) := d(\alpha_1, \ldots, \alpha_n) = \det(\tau_i \alpha_j)^2$., where τ_i runs over all the embeddings of K.

Definition 2.5. The above description of $d(\mathfrak{a})$ is called the *discriminant of the ideal* $\mathfrak{a}$. We define the *discriminant of the field* K to be $d_k := d(\mathcal{O}_K)$.

It is not immediately clear why this definition makes sense. That is, we need to check that $d(\mathfrak{a})$ is invariant under the choice of integral basis $\alpha_1, \ldots, \alpha_n$. Now, if $\alpha'_1, \ldots, \alpha'_n$ is another basis, then there is some $n \times n$ matrix T with determinant ± 1 such that $(\alpha'_1, \ldots, \alpha'_n)T = (\alpha_1, \ldots, \alpha_n)$, which means that, passing to matrices, $(\tau_i \alpha'_j)T = (\tau_i \alpha_j)$. Taking the square of the determinant of both sides, we get $(\det T)^2 d(\alpha'_1, \ldots, \alpha'_n) = d(\alpha_1, \ldots, \alpha_n)$. Hence we have shown that the discriminant is well-defined.

Theorem 2.4. *If $0 \neq \mathfrak{a} \lhd \mathcal{O}_K$, then $\Gamma = j\mathfrak{a}$ is a complete lattice in $K_{\mathbb{R}}$ and vol$(\Gamma) = \sqrt{|d_K|}[\mathcal{O}_K : \mathfrak{a}]$.*

Remark. If Γ is a complete lattice with basis $v_1, \dots, v_n$, then $\Phi = \{x_1v_1 + \cdots + x_nv_n : 0 \leq x_i < 1\}$ is the fundamental domain. Then $\mathrm{vol}(\Gamma) = \mathrm{vol}(\Phi) = |\det(A)|$, where A be the $n \times n$ matrix satisfying

$$\begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} = A \begin{pmatrix} e_1 \\ \vdots \\ e_n \end{pmatrix}.$$

Now, $AA^T = (\langle v_i, v_j \rangle)_{i,j}$, so then we get $\mathrm{vol}(\Gamma) = |\det(A)| = \sqrt{|det(\langle v_i, v_j \rangle)|}$.

As a slight tangent, we mention discuss the notion of a fundamental domain. We have thrown around these words in our discussion of lattices, but we haven't actually defined what these words mean. It happens that we can view Γ as a set acting on our vector space V. Then we can say that two points $\alpha, \beta \in V$ are equivalent (we write $\alpha \sim \beta$ if $\alpha = \beta^\gamma$ for some $\gamma \in \Gamma$ (i.e. α is the Γ-image of β). Then the *fundamental domain* is a complete set of representatives of this equivalence relation. As we would expect, two fundamental domains have the same volume. Also, if $\Phi \subseteq V$ is a fundamental domain, then the disjoint union $\amalg_{\gamma \in \Gamma} \gamma\Phi = V$.

Now we prove a theorem which will allow us to prove Theorem 2.4 more easily.

Theorem 2.5. *Let $0 \neq \mathfrak{a} \subseteq \mathfrak{a}'$ be two finitely generated $\mathcal{O}_K$-submodules of K. Then we have $d(\mathfrak{a}) = [\mathfrak{a}' : \mathfrak{a}]^2 d(\mathfrak{a}')$.*

Proof. Let $\alpha_1, \dots, \alpha_n$ be a basis of $\mathfrak{a}$ and $\alpha_1', \dots, \alpha_n'$ a basis of $\mathfrak{a}'$. Then for some $n \times n$ matrix T (with integer entries and a nonzero determinant), we have $(\alpha_1', \dots, \alpha_n')T = (\alpha_1, \dots, \alpha_n)$. From this, we get that $d(\mathfrak{a}) = d(\mathfrak{a}')(\det T)^2$. We want to prove that $|\det T| = [\mathfrak{a}' : \mathfrak{a}]$.

Let Φ be a fundamental domain of $\mathfrak{a}$ and let Φ' be a fundamental domain of $\mathfrak{a}'$. Then $F\Phi' = \Phi$ so $|\det T|\mathrm{vol}(\Phi') = \mathrm{vol}(\Phi)$. From here, it is enough to show $[\mathfrak{a}' : \mathfrak{a}]\mathrm{vol}(\Phi') = \mathrm{vol}(\Phi)$. If Φ' is a fundamental domain of a', then $\amalg_{i \in I} \alpha_i \Phi'$ is a fundamental domain of $\mathfrak{a}$. Then

$$V = \amalg_{\alpha' \in \mathfrak{a}'} \alpha' \Phi' = \amalg_{i \in I} \amalg_{\alpha \in \mathfrak{a}} \alpha_i \alpha \Phi' = \amalg_{\alpha \in \mathfrak{a}} \alpha \left(\amalg_{i \in I} \alpha_i \Phi' \right).$$

So $\mathrm{vol}(\Phi) = \mathrm{vol}(\amalg_i \alpha_i \Phi') = |I|\mathrm{vol}(\Phi') = [\mathfrak{a}' : \mathfrak{a}]\mathrm{vol}(\Phi')$. This completes the proof. □

Now we can prove Theorem 2.4.

Proof of Theorem 2.4. Let $\alpha_1, \dots, \alpha_n$ be a $\mathbb{Z}$-basis of $\mathfrak{a}$. Then $\Gamma = \mathbb{Z}j\alpha_1 + \cdots + \mathbb{Z}j\alpha_n$ and $\mathrm{vol}(\Gamma)^2 = \det(\langle j\alpha_i, j\alpha_k \rangle)$, where $\langle j\alpha_i, j\alpha_k \rangle = \sum_{l=1}^n \tau_l \alpha_i \cdot \overline{\tau_l \alpha_k}$, $\tau_l : K \to \mathbb{C}$. Let $B := (\tau_l \alpha_i$. Then $B\overline{B^T} = (\langle j\alpha_i, j\alpha_k \rangle)$. This gives us

$$\mathrm{vol}(\Gamma)^2 = \det(B\overline{B^T}) = |\det(B)|^2 = |d(\mathfrak{a})|,$$

where the last equality holds by definition of the discriminant of an ideal. By Theorem 2.5, $d(\mathfrak{a}) = [\mathcal{O}_K : \mathfrak{a}]^2 d_K$, so $\mathrm{vol}(\Gamma)^2 = [\mathcal{O}_K : \mathfrak{a}]^2 d_K$. Taking the square root of both sides gives us the desired result, $\mathrm{vol}(\Gamma) = [\mathcal{O}_K : \mathfrak{a}]\sqrt{|d_K|}$. □

Question to ask Professor Biro during office hours: Where does the following theorem come from? Why is it useful? What does it say? Can we draw a picture?

For a reference, this theorem can be found on page 32 of Neukirch's book.

Theorem 2.6. *Let $0 \neq \mathfrak{a} \lhd \mathcal{O}_K$. Let $c_\tau > 0$ be real numbers such that for every $\tau \in Hom(K, \mathbb{C})$, we have $c_\tau = c_{\overline{\tau}}$. Assume that*

$$\prod_\tau c_\tau > A[\mathcal{O}_K : \mathfrak{a}],$$

where $A = (\frac{2}{\pi})^s \sqrt{|d_K|}$. Then there exists $0 \neq \alpha \in \mathfrak{a}$ such that $|\tau\alpha| < c_\tau$ for all $\tau \in Hom(K, \mathbb{C})$.

Proof. Let $X := \{(z_\tau) \in K_{\mathbb{R}} : |z_\tau| < c_\tau\}$. This set is centrally symmetric and convex. If we can prove that $\mathrm{vol}(X) > 2^n \mathrm{vol}(\Gamma)$, then we're done (since by Minkowski, there is a nonzero $\alpha \in \mathfrak{a}$ such that $j\alpha \in X$.) So what we need to prove is that $\mathrm{vol}(X) > 2^n \sqrt{|d_K|}[\mathcal{O}_K : \mathfrak{a}]$.

In the image of X in $\prod_\tau \mathbb{R}$, we have these conditions: $|x_\rho| < c_\rho, x_\sigma^2 + x_{\overline{\sigma}}^2 < c_\sigma^2$, where ρ runs over all the real embeddings of K and the pair $\sigma, \overline{\sigma}$ runs over all the pairs of complex embeddings of K. Thus, we have

$$\mathrm{vol}(X) = (\prod_\rho 2c_\rho)(\prod_\sigma \pi c_\sigma^2)2^s = 2^{r+s}\pi^s \prod_\tau c_\tau.$$

By substitution, we have

$$\mathrm{vol}(X) = 2^{r+s}\pi^s \prod_\tau c_\tau > 2^{r+s}\pi^s \left(\frac{2}{\pi}\right)^s \sqrt{|d_K|}[\mathcal{O}_K : \mathfrak{a}] = 2^n \sqrt{|d_K|}[\mathcal{O}_K : \mathfrak{a}].$$

By the parenthetical remark made earlier, this completes the proof. □

Now we finish the ultimate goal of all this machinery: to prove that the class number is finite. We write a few definitions, state some properties (without proof, for now), and then proceed to prove this (quite incredible!) theorem.

Definition 2.6. Consider a nonzero ideal $\mathfrak{a} \lhd \mathcal{O}_K$. Then the *norm of the ideal* is $N(\mathfrak{a}) := [\mathcal{O}_K : \mathfrak{a}]$.

It turns out that if we take a nonzero element $\alpha \in \mathcal{O}_K$, then $N((\alpha)) = |N_{K/\mathbb{Q}}(\alpha)|$. Also, if we have nonzero ideals $\mathfrak{a}, \mathfrak{b} \lhd \mathcal{O}_K$, then $N(\mathfrak{ab}) = N(\mathfrak{a})N(\mathfrak{b})$. Since every fractional ideal is of the form $\mathfrak{p}_1^{n_1} \cdots \mathfrak{p}_t^{n_t}$, where $\mathfrak{p}_i$ are prime ideals and n_i are nonzero integers (not necessarily positive), then we can write extend the definition of an integer ideal to work for fractional ideals; i.e. $N(\mathfrak{p}_1^{n_1} \cdots \mathfrak{p}_t^{n_t}) = N(\mathfrak{p}_1)^{n_1} \cdots N(\mathfrak{p}_t)^{n_t}$.

We state a lemma.

Lemma 2.1. *In every nonzero ideal $\mathfrak{a} \lhd \mathcal{O}_K$, there exists $0 \neq \alpha \in \mathfrak{a}$ such that*

$$|N_{K/\mathbb{Q}}(\alpha)| \leq (\frac{2}{\pi})^s \sqrt{|d_K|} N(\mathfrak{a}).$$

Proof. By the proof of Theorem 2.6, for every $\varepsilon > 0$, we can take c_τ ($\tau \in \mathrm{Hom}(K, \mathbb{C})$) such that $c_\tau = c_{\overline{\tau}}$ for every τ and $\prod_\tau c_\tau = (\frac{2}{\pi})^s \sqrt{|d_K|} N(\mathfrak{a}) + \varepsilon$. Also by the previous theorem, we know that there is some $0 \neq \alpha \in \mathfrak{a}$ such that $|\tau\alpha| < c_\tau$, and then taking the product, we get

$$|N_{k/\mathbb{Q}}(\alpha)| = |\prod_\tau \tau\alpha| < (\frac{2}{\pi})^s \sqrt{|d_K|} N(\mathfrak{a}) + \varepsilon.$$

Since this is true for all $\varepsilon > 0$ and since $|N_{K/\mathbb{Q}}(\alpha)|$ is always a positive integer, then there must be some $\alpha \in \mathfrak{a}$ satisfying

$$|N_{K/\mathbb{Q}}(\alpha)| \leq (\frac{2}{\pi})^s \sqrt{|d_K|} N(\mathfrak{a}),$$

the desired inequality. □

Now we can prove that the class number is finite. Recall first that the class number is the size of the ideal class group $Cl_K = J_K/P_K$, where J_K is the abelian group of fractional ideals and P_K is the subgroup of J_K consisting of principal fractional ideals.

Theorem 2.7. *The ideal class group $Cl_K = J_K/P_K$ is finite.*

Proof. We first prove that for any $M > 0$, then there are only finitely many $\mathfrak{a} \lhd \mathcal{O}_K$ with $N(\mathfrak{a}) \leq M$. If $\mathfrak{p} \lhd \mathcal{O}_K$, then $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$, where $\mathfrak{p}$ is a prime ideal and p is a rational prime. Then $\mathcal{O}_K/\mathfrak{p}$ is a finite field that is a finite field extension of $\mathbb{Z}/p\mathbb{Z}$. So $N(\mathfrak{p}) = |\mathcal{O}_K/\mathfrak{p}| = p^f$, where $f \geq 1$ is an integer, so in particular, $N(\mathfrak{p}) \geq p$. This inequality gives us that if $N(\mathfrak{p})$ is bounded, then p is also bounded, so there are only finitely many such p. The last step is to show that for a given p, there are only finitely many such $\mathfrak{p}$.

Notice that we must have $\mathfrak{p} \,|\, (p)$. Therefore it is enough to prove that each class of Cl_K contains an integral ideal with norm at most $(\frac{2}{\pi})^s \sqrt{|d_K|}$. (Note here that this gives us a method to determine the class number because then we only have finitely many cases to consider.) Let $\mathfrak{a}$ be a fractional ideal. Then there is an element $0 \neq \gamma \in \mathcal{O}_K$ such that $\gamma\mathfrak{a}^{-1} \subseteq \mathcal{O}_K$. We apply the lemma. Then there is some $0 \neq \alpha \in j\mathfrak{a}^{-1}$ such that

$$|N((\alpha))| = |N_{K/\mathbb{Q}}(\alpha)| \leq (\frac{2}{\pi})^s \sqrt{|d_K|} N(j\mathfrak{a}^{-1}).$$

Now, dividing, we get $N(\frac{(\alpha)}{j\mathfrak{a}^{-1}}) \leq (\frac{2}{\pi})^s\sqrt{|d_K|}$. The division in $\frac{(\alpha)}{j\mathfrak{a}^{-1}} = \mathfrak{a}\frac{(\alpha)}{j}$ takes place in J_K and to finish this off, let $\mathfrak{b} := \mathfrak{a}(\frac{\alpha}{j})$. Then since $j\mathfrak{a}^{-1}$ divides (α), then $\alpha \in j\mathfrak{a}^{-1}$, so $\mathfrak{b}$ is an integral ideal, and it is in the same class as $\mathfrak{a}$ and furthermore, $N(\mathfrak{b}) \leq (\frac{2}{\pi})^s\sqrt{|d_K|}$. This completes the proof that the ideal class group is finite. □

3. Cyclotomic Fields and Fermat: 6 - 13 October 2010

Over the next few lectures, we will build up the theory required to prove a special case of Fermat's Last Theorem. We state the proposition here.

Theorem 3.1. *Let p be a prime rational integer and consider the equation $x^p + y^p = z^p$ where $(p, xyz) = 1$ and $p \nmid h(\mathbb{Q}(\zeta_p))$.*

Here, $h(\mathbb{Q}(\zeta_p))$ denotes the class number of the cyclotomic field $\mathbb{Q}(\zeta_p)$ and ζ_p denotes a pth root of unity. We will develop some theory about pth cyclotomic fields and ultimately use this to prove Theorem 3.1. We take a moment to mention some notation. We will write ζ to denote the pth root of unity and let $K := \mathbb{Q}(\zeta)$.

Theorem 3.2. *Let r, s be rational integers with $(rs, p) = 1$. Then $\frac{\zeta^r - 1}{\zeta^s - 1}$ is a unit in $\mathbb{Z}[\zeta]$.*

Proof. There is an integer R such that $R \equiv r \pmod{p}, R \equiv 0 \pmod{s}$. Then

$$\frac{\zeta^r - 1}{\zeta^s - 1} = \frac{\zeta^R - 1}{\zeta^s - 1} = 1 + \zeta^s + \zeta^{2s} + \cdots + \zeta^{R-s} \in \mathbb{Z}[\zeta].$$

This completes the proof. □

Theorem 3.3. *The ideal $(1 - \zeta)$ is a prime ideal in K and $(1 - \zeta)^{p-1} = (p)$.*

Proof. □

Theorem 3.4. *The ring of integers of K is $\mathbb{Z}[\zeta]$; i.e. $\mathcal{O}_K = \mathbb{Z}[\zeta]$.*

Proof. We will use the fact from Theorem 3.3 that the ideal $(1-\zeta)$ is prime. Let us take a moment to discuss notation. If we have a nonzero $\beta \in K$, then $(\beta) = \mathfrak{p}_1^{n_1} \cdots \mathfrak{p}_t^{n_t}$, where $n_i \in \mathbb{Z}$ for each i. Now let $v_{\mathfrak{p}}(\beta)$ be the exponent of $\mathfrak{p}$ in the prime decomposition of β. We can say some things about the exponent. If $\beta_1, \beta_2 \in K \backslash \{0\}$ and $v_{\mathfrak{p}}(\beta_1) \neq v_{\mathfrak{p}}(\beta_2)$, then $v_{\mathfrak{p}}(\beta_1 + \beta_2) = \min(v_{\mathfrak{p}}(\beta_1), v_{\mathfrak{p}}(\beta_2))$. We know that $1, \zeta, \ldots, \zeta^{n-2}$ is a $\mathbb{Q}$-basis of K, so every $\alpha \in \mathcal{O}_K$ can be written in the form

$$\alpha = a_0 + a_1\zeta + \cdots + a_{p-2}\zeta^{p-2}, a_i \in \mathbb{Q}.$$

We will first prove that there is no p-power in the denominator of a_i for $0 \leq i \leq p - 2$.

Our first trick is to write α as a polynomial in $1 - \zeta$. Then we have

$$\alpha = b_0 + b_1(1 - \zeta) + \cdots + b_{p-2}(1 - \zeta)^{p-2}.$$

Notice that if each b_i has the property that there is no power of p in the denominator, then each a_i must also have this property, and the same is true in the reverse direction. Hence what we now want to show is that for an arbitrary .....

CONFUSED!!! Is the notation supposed to be $v_{\mathfrak{p}}(\beta)$??? Or is it supposed to be $v_p(\beta)$??? □

A treatment of this material can be found in Washington's *An Introduction to Cyclotomic Fields.*

4. Multiplicative Minkowski and Dirichlet's Unit Theorem: 19 - 26 October 2010

We first begin by introducing some new notation.

Let $\mathcal{O}_K^\times$ denote the group of units in $\mathcal{O}_K$ and $\mu(K)$ denote the group of roots of unity in K. It is clear that $\mu(K) \subseteq \mathcal{O}_K$. It will in fact turn out that we have the isomorphism

$$\mathcal{O}_K^\times \cong \mu(K) \times \mathbb{Z}^{r+s-1},$$

where as usual, r is the number of real embeddings and s is the number of complex conjugate pairs of embeddings (so we have $2s$ non-real complex embeddings). As an example, we can take the cyclotomic field $K = \mathbb{Q}(\zeta_p)$, and then $r = 0, s = \frac{p-1}{2}$. We state (without proof) the fact that $K_0 := \mathbb{Q}(\zeta_p + \overline{\zeta_p}) = K \cap \overline{K}$. So here, $s = 0, r = \frac{p-1}{2}$.

Now we turn to discuss the multiplicative version of Minkowski. Consider the homomorphism

$$j : K^\times \to K_{\mathbb{C}}^\times := \prod_\tau \mathbb{C}^\times, a \mapsto (\tau a), \tau \in \mathrm{Hom}(K, \mathbb{C}).$$

Here, $K^\times$ denotes the multiplicative group of K. We also have the norm homomorphism

$$N : K_{\mathbb{C}}^\times \to \mathbb{C}^\times = \mathbb{C}\backslash\{0\}, z = (z_\tau) \mapsto \prod_\tau z_\tau.$$

From this map, we get that $N(ja) = N_{K/\mathbb{Q}}(a)$ for $a \in K^\times$. Now define a homomorphism

$$l : \mathbb{C}^\times \to \mathbb{R}, z \mapsto \log|z|,$$

where we view $\mathbb{C}^\times$ as a multiplicative group and $\mathbb{R}$ as an additive group. It is easy to verify that this is indeed a homomorphism. This induces another homomorphism, which we also call l, with a bit of abuse of notation. So we have $l : K_{\mathbb{C}}^\times \to \prod_\tau \mathbb{R}$, where the image is dictated by the previous l, coordinate-wise.

The image of $K^\times$ by j is

$$K_{\mathbb{R}}^\times = \{(z_\tau) \in K_{\mathbb{C}}^\times : z_\rho \in \mathbb{R}, z_{\overline{\sigma}} = \overline{z}_\sigma\},$$

where ρ runs over the real embeddings $\rho_1, \ldots, \rho_r$ and σ runs over the complex embeddings $\sigma_1, \ldots, \sigma_s$ (with each σ_i a representative from a pair of conjugate complex embeddings). The image of $K_{\mathbb{R}}^\times$ by l is in

$$[\prod_\tau \mathbb{R}]^+ := \prod_\rho \mathbb{R} \times \prod_\sigma [\mathbb{R} \times \mathbb{R}]^+, \text{ where } [\mathbb{R} \times \mathbb{R}]^+ := \{(x, x) \in \mathbb{R} \times \mathbb{R} : x \in \mathbb{R}\}.$$

We have an isomorphism $[\prod_\tau \mathbb{R}]^+ \cong \mathbb{R}^{r+s}$ where we take the identity on $\prod_\rho \mathbb{R}$ and take the isomorphism $[\mathbb{R} \times \mathbb{R}]^+ \to \mathbb{R}, (x, x) \mapsto 2x$. Summarizing, we have

$$j : K^\times \to K_{\mathbb{R}}^\times, \text{ and } l : K_{\mathbb{R}}^\times \to [\prod \mathbb{R}]^+ \cong \mathbb{R}^{r+s}.$$

So if we take $x \in K_{\mathbb{R}}^\times$, we can write out the map l explicitly as follows:

$$l(x) = (\log|x_{\rho_1}|, \ldots, \log|x_{\rho_r}|, \log|x_{\sigma_1}|^2, \ldots, \log|x_{\sigma_s}|^2).$$

Notice here that we have the square of the log for the complex embeddings since in the isomorphism $[\prod_\tau \mathbb{R}]^+ \cong \mathbb{R}^{r+s}$, we took the map $[\mathbb{R} \times \mathbb{R}]^+ \to \mathbb{R}, (x, x) \mapsto 2x$, and also $\log|x|^2 = 2\log|x|$. From this, the following proposition becomes trivial.

Proposition 4.1. *Let $\alpha \in \mathcal{O}_K^\times$. Then $l(j\alpha) = 0 \in \mathbb{R}^{r+s}$ if and only if $\alpha \in \mu(K)$.*

Proof. The direction ($\Leftarrow$) is trivial from the definition. The direction ($\Rightarrow$) follows from the previous lemma stating that if $\alpha \in \mathcal{O}_K$ is such that every Galois conjugate of α has absolute value 1, then α must be a root of unity. □

It will in fact turn out that $l(j\mathcal{O}_K^\times)$ is a lattice in $\mathbb{R}^{r+s}$. It cannot be a complete lattice, however, since the restriction of l to the ring of integers $\mathcal{O}_K^\times$ has a nontrivial intersection. But it turns out that it is a complete lattice in an $r + s - 1$-dimensional subspace of $\mathbb{R}^{r+s}$. We discuss this more in the following class.

[20 October 2010] Recall from last class that we proved $[\prod_\tau \mathbb{R}]^+ \cong \mathbb{R}^{r+s}$. Now let us consider the map $\mathrm{Tr} : \mathbb{R}^{r+s} \to \mathbb{R}$ defined by summing the coordinates. Let $H := \{x \in \mathbb{R}^{r+s} : \mathrm{Tr}(x) = 0\}$.

Remark. If $\alpha \in \mathcal{O}_K^\times, |N_{K/\mathbb{Q}}(\alpha)| = 1$, then $l(j\alpha) \in H$. (This is true for every $\alpha \in K^\times$.) This is easy to see by just writing out the coordinates of $l(j\alpha)$ explicitly. We have $l(j\alpha) = (\log|\rho_1\alpha|, \dots, \log|\rho_r\alpha|, \log|\sigma_1\alpha|^2, \dots, \log|\sigma_s\alpha|^2)$, so $\mathrm{Tr}(l(j\alpha)) = \log|N_{K/\mathbb{Q}}(\alpha)| = 0$.

We now state the main theorem of this section. Once we have proven this theorem (which will take most of this section), Dirichlet's Unit Theorem can be easily deduced.

Theorem 4.1. $\Gamma := l(j\mathcal{O}_K^\times)$ *is a complete lattice in* H.

As of now, all we know is that $\Gamma \subseteq H$. Recall from earlier that a complete lattice is a free abelian group with a maximal number of generators. So here, since H is a $(r+s-1)$-dimensional space, then our ultimate goal will be to prove that Γ is a free abelian group with $r+s-1$ generators. To prove this theorem, we will need several lemmas.

Lemma 4.1. *Let a be a nonzero rational integer. Up to multiplication by units, there are only finitely many elements of $\alpha \in \mathcal{O}_K$ such that $N_{K/\mathbb{Q}}(\alpha) = a$.*

Proof. If $N_{K/\mathbb{Q}}(\alpha_1) = N_{K/\mathbb{Q}}(\alpha_2) = a$ and $\alpha_1 = \alpha_2 + a\gamma, \gamma \in \mathcal{O}_K$, then $\frac{\alpha_1}{\alpha_2} = 1 + \frac{a}{\alpha_2}\gamma \in \mathcal{O}_K$. But the same is true for $\frac{\alpha_2}{\alpha_1}$, so $\frac{\alpha_1}{\alpha_2}$ must be a unit. So we have proven that if α_1, α_2 have norm a and if $\alpha_1 \equiv \alpha_2 \pmod{a\mathcal{O}_K}$, then $\frac{\alpha_1}{\alpha_2}$. Since there are only finitely many elements of the factor ring $\mathcal{O}_K/(a)\mathcal{O}_K$, then the desired result follows. □

Definition 4.1. We say that $\Gamma \subseteq \mathbb{R}^m$ is a *discrete subgroup* of $\mathbb{R}^m$ if every point of Γ has a neighborhood containing no other point of Γ.

Lemma 4.2. Γ *is a lattice in* $\mathbb{R}^m$ *if and only if it is a discrete subgroup of* $\mathbb{R}^m$.

Proof. The forward direction ($\Rightarrow$) is trivial. For the reverse direction, we first prove that Γ is closed in V. Suppose $x \notin \Gamma$ but it is in the closure of Γ. Then for all $\varepsilon > 0$, we have $\gamma_1 \neq \gamma_2$, $\gamma_1, \gamma_2 \in \Gamma$ such that $|\gamma_1 - x| < \varepsilon, |\gamma_2 - x| < \varepsilon$ which implies that $0 < |\gamma_1 - \gamma_2| < 2\varepsilon$, which is a contradiction to the fact that Γ is discrete. Hence Γ must be closed.

Now let V_0 be the (real) subspace generated by Γ in V. Let $m := \dim V_0 \leq \dim V =: n$. Let $u_1, \dots, u_m \in \Gamma$ be a basis of V_0. Let $\Gamma := \mathbb{Z}u_1 + \cdots + \mathbb{Z}u_m$. This is a lattice. Clearly $\Gamma_0 \leq \Gamma$. It is enough to show that Γ_0 has finite index in Γ since if this is true, then letting $q := [\Gamma : \Gamma_0]$, we have $q\Gamma \leq \Gamma_0$, which implies that we have $\Gamma_0 \leq \Gamma \leq \frac{1}{q}\Gamma_0$. Since Γ_0 and $\frac{1}{q}\Gamma_0$ are free abelian groups of rank m, then Γ must also be, and hence it is a lattice of rank m.

So we have left to prove that Γ_0 has finite index in Γ. Let Φ_0 be the fundamental domain of Γ_0 in V_0. Then Φ_0 is bounded and $\Phi_0 + \Gamma_0 = V_0$. Then using the fact that $\Gamma \subseteq V_0$, then for every $\gamma \in \Gamma$, we have a representation $\gamma = \mu + \gamma_0$, where $\mu \in \Phi_0$ and $\gamma_0 \in \Gamma_0$. This implies that we have $\mu = \gamma - \gamma_0 \in \Gamma \cap \Phi_0$, so $\mu \in \mathrm{cl}(\Phi_0) \cap \Gamma$. Now, $\mathrm{cl}(\Phi_0) \cap \Gamma$ is closed since Γ is closed, and this is also a discrete set, since it is a subset of Γ. Also, it is bounded. This implies that $\mathrm{cl}(\Phi_0) \cap \Gamma$ is compact. Since compactness together with discreteness implies finiteness, then we have, finally, that $\mathrm{cl}(\Phi_0) \cap \Gamma$ is finite. It follows that Γ_0 has finite index in Γ. □

This lemma tells us that we want to prove that Γ is a discrete subgroup. In fact, since we have $\Gamma \subseteq H \subseteq \mathbb{R}^{r+s} \cong [\prod_\tau \mathbb{R}]^+ \subseteq \prod_\tau \mathbb{R}$, it is enough to prove the following.

Lemma 4.3. *For any $c > 0$, the set $\{(x_\tau) \in \prod_\tau \mathbb{R} : |x_\tau| \leq c\}$ contains only finitely many elements of Γ.*

Proof. If $\alpha \in \mathcal{O}_K^\times$, then $l(j\alpha)$ is in this set if and only if $e^{-c} \leq |\tau\alpha| \leq e^c$ for every $\tau \in \mathrm{Hom}(K, \mathbb{C})$. This puts a bound on the coefficients of the minimal polynomial of α (since the coefficients are just sums and products of the Galois conjugates $\tau\alpha$ of α). Hence there are only finitely many such polynomials, which means there can only be finitely many such α. Hence this set only has finitely many elements. □

We deduce from this lemma that Γ is a discrete subgroup, and by Lemma 4.2, this means that Γ is a lattice. It remains to be shown that Γ is a complete lattice of H. We introduce now the final lemma before we prove Theorem 4.1.

Lemma 4.4. *If $\Gamma \subseteq \mathbb{R}^m$ is a lattice, and $M \subseteq \mathbb{R}^m$ is a bounded set such that $M + \Gamma = \mathbb{R}^m$, then Γ is a complete lattice.*

Proof. The direction ($\Rightarrow$) is trivial, taking the fundamental domain as M. For the reverse direction, let V_0 be the subspace generated by Γ in V. This is a real subspace of V. We want to show that $V_0 = V$. Take $v \in V$. Then for any $m \in \mathbb{Z}$, we can write $mv = a_m + \gamma_m$ for some $a_m \in M, \gamma_m \in \Gamma$. Solving for v, we get $v = \frac{a_m}{m} + \frac{r_m}{m}$. The first term tends to 0 as m tends to infinity since $a_m \in M$ and M is a bounded set. The second term is an element of V_0, and v is in the topological closure of V_0. But since any real subspace is automatically closed, we have $v \in V_0$. Hence we have proven $V \subseteq V_0$, and so equality follows. □

Now we have everything we need to prove Theorem 4.1.

Proof of Theorem 4.1. We would like to construct such a set M for Γ. First, let $S := \{y \in K_{\mathbb{R}}^{\times} : |N(y)| = 1\}$. Recall the map $j : K^{\times} \to K_{\mathbb{R}}^{\times} \subseteq K_{\mathbb{R}}$. We will construct a subspace $T \subseteq S$ such that T is bounded in $K_{\mathbb{R}}$ and $S = \cup_{\varepsilon \in \mathcal{O}_K^{\times}} T \cdot j\varepsilon$. Then $M = l(T)$ will be a set that satisfies Lemma 4.4 for Γ. Why is this so? Well, first it is easy to see that $l(S) = H$. Then we have

$$H = l(S) = \bigcup_{\varepsilon \in \mathcal{O}_K^{\times}} l(T)l(j\varepsilon) = \bigcup_{\gamma \in \Gamma} l(T)\gamma = \bigcup_{\gamma \in \Gamma} M\gamma,$$

and hence $H = M + \Gamma$. Also, since $T \subseteq S$, then T is bounded, and hence $l(T)$ must also be bounded. Therefore, once we have constructed such a set T, then we can define M based on this set, by Lemma 4.4, Γ is a complete lattice of H. So let's construct T.

Recall from Minkowski Theory the following theorem: If $c_\tau > 0$ for $\tau \in \mathrm{Hom}(K, \mathbb{C}), c_\tau = c_{\overline{\tau}}$ and $\prod_\tau c_\tau > (\frac{2}{\pi})^s \sqrt{|d_K|} N(\mathfrak{a})$, where $0 \neq \mathfrak{a} \lhd \mathcal{O}_K$, then there is a nonzero $\alpha \in \mathfrak{a}$ such that $|\tau\alpha| < c_\tau$ (Theorem 2.6). We apply this to the case when we have $\mathfrak{a} = \mathcal{O}_K$. Let c_τ be as above, and let $C := \prod_\tau c_\tau > (\frac{2}{\pi})^s \sqrt{|d_K|}$. Now define a set

$$X := \{(z_\tau) \in K_{\mathbb{R}} : |z_\tau| < c_\tau\}.$$

Then by Theorem 2.6 (stated above), there exists a nonzero $\alpha \in \mathcal{O}_K$ such that $j\alpha \in X$. (Recall from earlier, in Minkowski Theory, that j is a map that whose image in $K_{\mathbb{R}}$ is defined by an ordered n-tuple, each coordinate of which is the image of the original point under some embedding of the number field K.) Now let us take $y = (y_\tau) \in S$. Then we define Xy to be a similar set:

$$Xy := \{(z_\tau) \in K_{\mathbb{R}} : |z_\tau| < c_\tau \cdot |y_\tau| \text{ for all } \tau \in \mathrm{Hom}(K, \mathbb{C})\}.$$

Notice that since $y \in S$, then the product of over all $\tau \in \mathrm{Hom}(K, \mathbb{C})$ of $c_\tau \cdot |y_\tau| = C$. Again by Theorem 2.6, there exists a nonzero $\alpha \in \mathcal{O}_K$ such that $j\alpha \in Xy$, so $j\alpha = xy$ for some $x \in X$, which means, rearranging terms, that $y^{-1} = x(j\alpha)^{-1}$.

(Notice that this is quite close to what we want to prove: We have now that any element of S can be written as $x(j\alpha)^{-1}$, that is, the product of an element from a bounded set and some element of $K_{\mathbb{R}}$. In order to prove $S = \cup_{\varepsilon \in \mathcal{O}_K^{\times}} T \cdot \gamma\varepsilon$, we need to show that we can replace $(j\alpha)^{-1}$ with an element of norm 1.)

By a previous lemma, if we know that there are $\alpha_1, \ldots, \alpha_N \in \mathcal{O}_K$ such that for every $\alpha \in \mathcal{O}_K$ having $|N_{K/\mathbb{Q}}(\alpha)| < C$, then we have a representation $\varepsilon\alpha = \alpha_i$ for some $\varepsilon \in \mathcal{O}_K$. Applying this, we have

$$y^{-1} = x(j\alpha)^{-1} = x(j\alpha^{-1}) = xj(\varepsilon\alpha_i^{-1}) = xj(\varepsilon)j(a_i^{-1}),$$

and since $y^{-1} \in S, j(\varepsilon) \in S$, then $xj(\alpha)^{-1} \in S$. It follows then that

$$S = \bigcup_{\varepsilon \in \mathcal{O}_K^{\times}} \left(\bigcup_{i=1}^{N} (S \cap Xj(\alpha_i^{-1})) \right) j(\varepsilon).$$

Now let $T := \cup_{i=1}^{N} (S \cap Xj\alpha_i^{-1})$. T is bounded in $K_{\mathbb{R}}$, since S is bounded and the boundedness of $Xj\alpha_i^{-1}$ follows from the boundedness of X. Therefore, by Lemma 4.4, Γ is a complete lattice. □

Now we can state and prove Dirichlet's Unit Theorem.

Theorem 4.2 (Dirichlet's Unit Theorem.)**.** *The group of units $\mathcal{O}_K^\times$ of $\mathcal{O}_K$ is the direct product of the finite cyclic group $\mu(K)$ and a free abelian group of rank $r+s-1$.*

Proof. Let $\lambda = l \circ j$. Then since $\Gamma = \lambda(\mathcal{O}_K^\times)$, the map $\lambda : \mathcal{O}_K^\times \to \Gamma \cong \mathbb{Z}^{r+s-1}$ is a surjective group homomorphism and with $\ker \lambda = \mu(K)$. Let $\gamma_1, \gamma_2, \ldots, \gamma_{r+s-1}$ be a free system of generators of Γ. Let $\varepsilon_1, \ldots, \varepsilon_{r+s-1}$ be such that $\lambda\varepsilon_i = \gamma_i$ (i.e. $\varepsilon_1, \ldots, \varepsilon_{r+s-1}$ are the preimages.) Then

$$\mu(K) \cap \varepsilon_1^{\mathbb{Z}} \cdot \varepsilon_2^{\mathbb{Z}} \cdots \varepsilon_{r+s-1}^{\mathbb{Z}} = \{1\} \Rightarrow \mu(K) \cdot \varepsilon_1^{\mathbb{Z}} \cdot \varepsilon_2^{\mathbb{Z}} \cdots \varepsilon_{r+s-1}^{\mathbb{Z}} = \mathcal{O}_K^\times,$$

where $\varepsilon_i^{\mathbb{Z}}$ denotes any integer power of ε_1. Hence there exist elements $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{r+s-1} \in \mathcal{O}_K^\times$ such that every $\varepsilon \in \mathcal{O}_K^\times$ can be uniquely written in the form

$$\varepsilon = \zeta \cdot \varepsilon_1^{m_1} \cdots \varepsilon_{r+s-1}^{m_{r+s-1}}, \text{ where } \zeta \in \mu(K) \text{ and } m_1, \ldots, m_{r+s-1} \in \mathbb{Z}.$$

The units $\varepsilon_1, \ldots, \varepsilon_{r+s-1}$ are called *fundamental units.* □

Let us now introduce the concept of a regulator of a field K. Recall the map $\lambda : \mathcal{O}_K^\times \to H \subseteq \mathbb{R}^{r+s}$. We proved that $\Gamma := \lambda(\mathcal{O}_K^\times)$ is a complete lattice. It has a fundamental domain. The regulator is related to the ..... of the fundamental domain. Now let us take a vector in $\mathbb{R}^{r+s}$ orthogonal to H. We will choose

$$\lambda_0 := \frac{1}{\sqrt{r+s}}(1, \ldots, 1) \in \mathbb{R}^{r+s}.$$

Then if $\varepsilon_1, \ldots, \varepsilon_{r+s-1}$ is a system of fundamental units, then $\lambda_0, \lambda(\varepsilon_1), \ldots, \lambda(\varepsilon_{r+s-1})$ is a basis of a complete lattice in $\mathbb{R}^{r+s}$. The fundamental domain of this lattice has volume:

$$d := \left| \det \begin{pmatrix} \frac{1}{\sqrt{r+s}} & \lambda(\varepsilon_1)_1 & \cdots & \lambda(\varepsilon_{r+s-1})_1 \\ \vdots & \vdots & \ddots & \vdots \\ \frac{1}{\sqrt{r+s}} & \lambda(\varepsilon_1)_{r+s} & \cdots & \lambda(\varepsilon_{r+s-1})_{r+s} \end{pmatrix} \right|.$$

If Φ is a fundamental domain of Γ in H, then $\mathrm{vol}(\Phi) = d$. We can compute d by adding all rows to the first row, which gives us:

$$d = \left| \det \begin{pmatrix} \sqrt{r+s} & 0 & \cdots & 0 \\ 0 & \lambda(\varepsilon_1)_2 & \cdots & \lambda(\varepsilon_{r+s-1})_2 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & \lambda(\varepsilon_1)_{r+s} & \cdots & \lambda(\varepsilon_{r+s-1})_{r+s} \end{pmatrix} \right|.$$

Therefore, letting the bottom right $(r+s-1) \times (r+s-1)$ matrix be A, we have $d = \sqrt{r+s}R$, where $R = |\det(A)|$. Collecting this information, we write the following definition:

Definition 4.2. The *regulator of K*, denoted R_K (this is R in the above analysis), is defined to be the absolute value of the determinant of any $(r+s-1) \times (r+s-1)$ minor of the matrix

$$\begin{pmatrix} \lambda(\varepsilon_1)_1 & \cdots & \lambda(\varepsilon_{r+s-1})_1 \\ \vdots & \ddots & \vdots \\ \lambda(\varepsilon_1)_{t+1} & \cdots & \lambda(\varepsilon_{r+s-1})_{r+s} \end{pmatrix}.$$

From our analysis above, we see that the regulator is well-defined; i.e. it is invariant under the choice of units and choice of minor, which follows since d is independent of the choice of the fundamental system of units and also choice of deletion. The explicit form of this matrix is:

$$\begin{pmatrix} \log|\rho_1(\varepsilon_1)| & \cdots & \log|\rho_1(\varepsilon_{r+s-1})| \\ \vdots & \ddots & \vdots \\ \log|\rho_r(\varepsilon_1)| & \cdots & \log|\rho_r(\varepsilon_{r+s-1})| \\ \log|\sigma_1(\varepsilon_1)|^2 & \cdots & \log|\sigma_1(\varepsilon_{r+s-1})|^2 \\ \vdots & \ddots & \vdots \\ \log|\sigma_s(\varepsilon_1)|^2 & \cdots & \log|\sigma_s(\varepsilon_{r+s-1})|^2 \end{pmatrix}.$$

Why is the regulator important? How do we make sense of this definition? What does this tell us?

5. Factoring Rational Primes in Algebraic Number Fields: 26 October 2010

This material is covered in part in Chapter 1, §8 of Neukirch's book. We will discuss the decomposition of prime ideals in larger algebraic number fields. For instance, if p is a rational prime and L is a finite extension of $\mathbb{Q}$, how does p decompose into prime ideals in the ring of integers $\mathcal{O}_L$? To explore this, we first introduce some notation.

Let $K \subseteq L$ be algebraic number fields. If $P \lhd \mathcal{O}_K$ is a prime ideal, then $P\mathcal{O}_L \lhd \mathcal{O}_L$ and we can write $P\mathcal{O}_L = Q_1^{e_1} \dots Q_r^{e_r}$, where Q_i are prime ideals in $\mathcal{O}_L$ and $e_i \geq 1, e_i \in \mathbb{Z}$. We call e_i the *ramification index* of Q_i. For each i, we have $Q_i \cap K = P$, and $Q \lhd \mathcal{O}_L$ is among the Q_i if and only if $Q \cap K = P$. Now consider the finite field k obtained by taking the quotient $\mathcal{O}_K/P =: k$. Then every $\mathcal{O}_K/Q_i$ can be viewed as a vector space over k. We denote its dimension by f_i and call this the *inertia degree* of Q_i. The prime ideal $Q_i \lhd \mathcal{O}_L$ is said to be *ramified* over K if $e_i > 1$. It is natural to extend this definition to P; i.e. we say the prime ideal $P \lhd \mathcal{O}_K$ is *ramified* if there is an i such that $e_i > 1$. It will turn out that there will only be finitely many ramified primes. Our first theorem will be a statement relating the ramification index e_i and the inertia degree f_i.

Theorem 5.1. *Using the notation above, $\sum_{i=1}^{r} e_i f_i = n$, where $n = [L : K]$.*

Proof. Let $P \lhd \mathcal{O}_K$ be a prime ideal with the following decomposition in $\mathcal{O}_L$: $P\mathcal{O}_L = Q_1^{e_1} \cdots !_r^{e_r}$. By the Chinese Remainder Theorem, we have

$$\mathcal{O}_L/P\mathcal{O}_L \cong \oplus_{i=1}^{r} \mathcal{O}_L/!_i^{e_i}.$$

On the RHS, the number of elements in each quotient $\mathcal{O}_L/Q(i^{e_i})$ is exactly the norm of $Q_i^{e_i}$. Now, $N(Q_i)^{e_i} = (|k|^{f_i})^{e_i}$, so the number of elements of the direct sum on the right is $|k|^{\sum e_i f_i}$. On the LHS, we have a vector space over k. Therefore to show that $\sum e_i f_i = n$, it is enough to show that $\mathcal{O}_L/P\mathcal{O}_L$ is an n-dimensional vector space over the finite field k.

Let $\omega_1, \dots, \omega_m \in \mathcal{O}_L$ be elements such that their images $\overline{\omega}_1, \dots, \overline{\omega}_m$ in $\mathcal{O}_L/P\mathcal{O}_L$ are independent over k. We claim that then $\omega, \dots, \omega_m$ are independent over K (so that $m \leq n$). Suppose that they are not independent. Then there exist $\alpha_i \in K$, not all 0, such that $\alpha_1\omega_1 + \cdots \alpha_m\omega_m = 0$. It is no loss to assume that $\alpha_i \in \mathcal{O}_K$ since we can always multiply through and clear denominators. Let us define an ideal $\mathfrak{a} := (\alpha_1, \dots, \alpha_m) \lhd \mathcal{O}_K$. We would like to find $\alpha \in K$ such that $\alpha\alpha_i \in \mathcal{O}_K$ are not all in P. (This will give us a contradiction.) We need an $\alpha \in K$ such that $(\alpha)\mathfrak{a} \subseteq \mathcal{O}_K, (\alpha)\mathfrak{a} \not\subseteq P$. Now, the second condition holds if and only if $(\alpha)\mathfrak{a}P^{-1} \not\subseteq \mathcal{O}_K$, so it is sufficient to find an $\alpha \in \mathfrak{a}^{-1} \backslash (\mathfrak{a}P^{-1})^{-1} = \mathfrak{a}^{-1} \backslash \mathfrak{a}^{-1}P$. Now, $\mathfrak{a}^{-1}P \subseteq \mathfrak{a}^{-1}$ since $\mathfrak{a}^{-1}$ is a fractional ideal, but $\mathfrak{a}^{-1}P \neq \mathfrak{a}^{-1}$ by unique prime factorization, and so $\mathfrak{a}^{-1} \backslash \mathfrak{a}^{-1}P$ is nonempty and the desired α can be found. Hence we can find an α such that

$$\alpha\alpha_1\omega_1 + \cdots + \alpha\alpha_m\omega_m \equiv 0 \pmod{P},$$

with not all $\alpha\alpha_1$ in P. This gives us a linear dependence among the $\overline{\omega}_1, \dots, \overline{\omega}_m$ over k (since the images of $\alpha\alpha_i$ are not all zero), and this is a contradiction. So we conclude that $\omega_1, \dots, \omega_m$ are linearly independent over K and $m \leq n$.

To prove the reverse inequality, let $\omega_1, \dots, \omega_m \in \mathcal{O}_L$ be such that $\overline{\omega}_1, \dots, \overline{\omega}_m$ is a basis of $\mathcal{O}_L/P\mathcal{O}_L$ over k. We will prove that $\omega_1, \dots, \omega_m$ is a basis of L over K. Let $M := \mathcal{O}_K\omega + \cdots + \mathcal{O}_K\omega_m$. This is an $\mathcal{O}_K$-module. Now, $M \subseteq \mathcal{O}_L$, and we can view $\mathcal{O}_L$ also as an $\mathcal{O}_K$-module. Now let $N := \mathcal{O}_L/M$, the quotient $\mathcal{O}_K$-module. We know that $\mathcal{O}_L = M + P\mathcal{O}_L$, so $N = PN \subseteq \mathcal{O}_L$, and since $\mathcal{O}_L$ is a finitely generated $\mathcal{O}_K$-module, then N must also be a finitely generated $\mathcal{O}_K$-module. Now let $x_1, \dots, x_t$ be a system of generators of N over $\mathcal{O}_K$. We can write $x_i = \sum_{j=1}^{t} \alpha_{ij}x_j$, where $\alpha_i j \in P$. In matrix form, these equations give

$$\begin{pmatrix} 1-\alpha_{11} & -\alpha_{12} & \cdots & -\alpha_{1t} \\ -\alpha_{21} & 1-\alpha_{22} & \cdots & -\alpha_{2t} \\ \vdots & \vdots & \ddots & \vdots \\ -\alpha_{t1} & -\alpha_{t2} & \cdots & 1-\alpha_{tt} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_t \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

Denote the $t \times t$ matrix by A and let $d := \det A$. Multiplying by the adjoint matrix of A, we see that $dx_i = 0$, so $dN = 0$. But $d \in \mathcal{O}_K \backslash P$ and $d \neq 0$. Since $N = \mathcal{O}_L/M$, then $d\mathcal{O}_L \subseteq M =$

$\mathcal{O}_K\omega_1 + \cdots + \mathcal{O}_K\omega_m$ and so $\mathcal{O}_L \subseteq K\omega_1 + \cdots + K\omega_m$ and $L \subseteq K\omega_1 + \cdots + K\omega_m$. This implies that $m \geq n$, and so this finishes the proof of the reverse inequality and we are done. $\square$

To sum up the above proof, we had two main steps: to prove that $\omega_1, \ldots, \omega_m$ are linearly independent over K and then to show that in fact $\omega_1, \ldots, \omega_m$ generate L over K.

This theorem is also known as the *fundamental identity.*

Consider now the separable extension $L|K$ given by the primitive element $\theta \in \mathcal{O}_L$ with minimal polynomial $F(X) \in \mathcal{O}_K[X]$ so that $L = K(\theta)$ and $[L : K] = n$. So $L = K(\theta)$. It is not guaranteed that $\mathcal{O}_L = \mathcal{O}_K[\theta]$. In general, all we know is $\mathcal{O}_K[\theta] \subseteq \mathcal{O}_L$, and it is a difficult problem in number theory to classify all fields L in which we can find a θ such that $1, \theta, \ldots, \theta^{n-1}$ is an integral basis. For now, we can only identify the decomposition of some primes P in $\mathcal{O}_L$. Here, an ideal called the conductor plays a large role. It is the largest ideal of $\mathcal{O}_L$ contained in $\mathcal{O}_K[\theta]$. We state a precise definition here.

Definition 5.1. The *conductor* of $\mathcal{O}_K[\theta]$ is

$$I := \{\alpha \in \mathcal{O}_L : \alpha\mathcal{O}_L \subseteq \mathcal{O}_K[\theta]\}.$$

Every element of L can be written as a K-linear combination of $1, \theta, \ldots, \theta^{n-1}$. We can clear denominators to get into $\mathcal{O}_K[\theta]$. This is true for every element of an integral basis of $\mathcal{O}_L$. In particular, we then get $I \neq 0$ since it contains a nonzero rational integer. Also note that in the case that $\mathcal{O}_K[\theta] = \mathcal{O}_L$, then the conductor agrees with the ring of integers of L, i.e. $I = \mathcal{O}_L$.

We now discuss the decomposition of prime ideals relatively prime to the conductor. First, a note about notation. If f is a polynomial over $\mathcal{O}_K$, then $\overline{f}$ is its reduction modulo P, so it is a polynomial over $k = \mathcal{O}_K/P$.

Theorem 5.2. *If $P \lhd \mathcal{O}_K$ is a prime ideal and $P\mathcal{O}_L$ is relatively prime to the conductor I, then we can determine explicitly the decomposition of $P\mathcal{O}_L$ using this θ in the following way. Let $\overline{F}(X) = \overline{F}_1(X)^{e_1} \cdots \overline{F}_r(X)^{e_r}$ be the irreducible decomposition in $k[X]$. Here, each $F_i(X) \in \mathcal{O}_K[X]$ has leading coefficient 1. Then $Q_i = P\mathcal{O}_L + F_i(\theta)\mathcal{O}_L$ for $1 \leq i \leq r$ are all the different prime ideals above P and we have $P\mathcal{O}_L = Q_1^{e_1} \cdots Q_r^{e_r}$ with inertia degree $f_i = \deg F_i$.*

What this theorem tells us is that the decomposition of prime ideals relatively prime to the conductor boils down to a question of the decomposition of the minimal polynomial in the larger field. Before proving this theorem, we first give some examples.

Example. Let $L = K(\sqrt{d}), K = \mathbb{Q}$, where d is a square free integer. If $d \equiv 2, 3 \pmod 4$, then letting $\theta = \sqrt{d}$, we have the minimal polynomial $F(X) = X^2 - d$ for θ. If $d \equiv 1 \pmod 4$, then let $\theta = \frac{1+\sqrt{d}}{2}$, and we have the minimal polynomial $F(X) = X^2 - X + \frac{1-d}{4}$ for θ. In the special case of quadratic extensions, $\mathcal{O}_L = \mathcal{O}_K[\theta]$, so $1, \theta$ is an integral basis. Now, $P = (p) \lhd \mathcal{O}_K = \mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$, so $k = \mathcal{O}_K/P \cong \mathbb{Z}/p\mathbb{Z}$.

Take $L = \mathbb{Q}(i)$. This is the case $d = -1$. We have to decompose $X^2 + 1$ modulo p. If $p = 2$, then $X^2 + 1 = (X + 1)^2 \pmod 2$, so 2 is the square of a prime ideal. If $p \equiv 1 \pmod 4$, then $X^2 + 1$ decomposes into 2 linear factors, so p will have 2 different prime ideal factors (this follows from the fact that -1 is a quadratic residue). If $p \equiv 3 \pmod 4$, then $X^2 + 1$ is irreducible (since -1 is not a quadratic residue), so p remains prime.

If $L = \mathbb{Q}(\zeta_p)$, then $1, \zeta_p, \ldots, \zeta_p^{p-2}$ is an integral basis, so, as in the case of quadratic extensions, we can use the theorem to determine all the prime ideals explicitly. We will do this later in these notes.

We now prove Theorem 5.2

Proof. We have a homomorphism $\mathcal{O}_K[\theta] \to \mathcal{O}_L/P\mathcal{O}_L$. (We take this by first injecting $\mathcal{O}_K[\theta]$ into $\mathcal{O}_L$ and then reducing modulo P.) We claim that this map is surjective. We first show that $\mathcal{O}_K[\theta] + P\mathcal{O}_L = \mathcal{O}_L$. Now, we know $\mathcal{O}_K[\theta] + P\mathcal{O}_L = \mathcal{O}_L$ since I and $P\mathcal{O}_L$ are relatively prime. Since $I \subseteq \mathcal{O}_K[\theta]$, then necessarily $\mathcal{O}_K[\theta] + P\mathcal{O}_L = \mathcal{O}_L$. What remains to be shown is that the kernel of this map os $P\mathcal{O}_K$. From the construction of the map, we know it has kernel $\mathcal{O}_K[\theta] \cap P\mathcal{O}_L$. So what we want to show is that $\mathcal{O}_K[\theta] \cap P\mathcal{O}_L = P\mathcal{O}_K[\theta]$. The containment $\supseteq$ is trivial. For the

reverse containment, we first claim that since $P\mathcal{O}_L$ and I are relatively prime, then P and $I \cap K$ are relatively prime.

We can write $I = R_1 R_2 \cdots R_l$ where R_i are prime ideals of $\mathcal{O}_L$. In the case when $K = \mathbb{Q}$, we have $N(I) \in I \cap K$, but $N(I) \notin P$ since otherwise we would have $N(I), N(P) \in P$, which would mean $1 \in P$ (since $N(R_i)$ is relatively prime $N(P)$). This implies that $P \not\supseteq I \cap K$, and so it follows from the fact that P is prime that P and $I \cap K$ are relatively prime. In the general case, we can see that $R_i \cap K \not\subseteq P$ since in the decomposition of $P\mathcal{O}_L$, we have every prime ideal lying above P. Let $\alpha_i \in R_i \cap K \backslash P$. Then $\prod_{i=1}^{l} \alpha_i \in I \cap K \backslash P$. So again, $P \not\supseteq I \cap K$, which means that P and $I \cap K$ are necessarily relatively prime.

So we have $P + I \cap K = \mathcal{O}_K$. Then

$$\mathcal{O}_K[\theta] \cap P\mathcal{O}_L \subseteq (P + I \cap K)(\mathcal{O}_K[\theta] \cap P\mathcal{O}_L) \subseteq P\mathcal{O}_K[\theta],$$

where the last containment is true since $I\mathcal{O}_L \subseteq \mathcal{O}_K[\theta]$ and so $(I \cap K)P\mathcal{O}_L \subseteq P\mathcal{O}_K[\theta]$. Hence we have proved that the described homomorphism $\mathcal{O}_K[\theta] \to \mathcal{O}_L/P\mathcal{O}_L$ is surjective and that $\ker(\mathcal{O}_K[\theta]/P\mathcal{O}_K[\theta] \to \mathcal{O}_L/P\mathcal{O}_L$ is an isomorphism. From the isomorphism theorems, we also have $\mathcal{O}_K[\theta]/P\mathcal{O}_K[\theta] \cong k[X]/\overline{F}(X)$. This means that the prime ideals of $\mathcal{O}_L$ containing $P\mathcal{O}_L$ are in a $1-1$ correspondence with the maximal ideals of $\mathcal{O}_L/P\mathcal{O}_L$. Now, $k[X]$ is a unique factorization domain, and the prime ideals here are the principal ideals generated by irreducible polynomials. In $k[X]/\overline{F}$, the maximal ideals are the images $(\overline{F}_i(X)) \lhd k[X]$, so the maximal ideals of $\mathcal{O}_L/P\mathcal{O}_L$ correspond to these ideals. Now, the index of $\overline{F}_i(X)$ in $k[X]$ is $|k|^{f_i}$. So if $Q_i \lhd \mathcal{O}_L$ corresponds to $(\overline{F}_i(X))$, then $N(Q_i) = |k|^{f_i}$, so Q_i is a prime ideal in $\mathcal{O}_L$ lying above P having inertia degree f_i. What remains to be shown is the concrete form of Q_i and the exponents. But this is just a matter of understanding what is happening. The following picture should help in understanding the correspondences between the ideals.

$$\begin{array}{ccccc}
\mathcal{O}_L/P\mathcal{O}_L & \xleftarrow{\sim} & \mathcal{O}_K[\theta]/P\mathcal{O}_K[\theta] & \xleftarrow{\sim} & k[X]/(\overline{F}(X)) \\
\cup\mathrm{I} & & \cup\mathrm{I} & & \cup\mathrm{I} \\
\mathrm{Im}(F_i(\theta) \lhd \mathcal{O}_L) & \longleftrightarrow & \mathrm{Im}((F_i(\theta)) \lhd \mathcal{O}_K[\theta]) & \longleftrightarrow & \mathrm{Im}((\overline{F}_i(X)) \lhd k[X]).
\end{array}$$

(In $\mathcal{O}_L/P\mathcal{O}_L$, the maximal ideals are the images of Q_i, the prime ideals containing $P\mathcal{O}_L$. If e_i is the maximal power of Q_i dividing $P\mathcal{O}_L$, then the images of $Q_i, Q_i^2, \ldots, Q_i^{e_i}$ in $\mathcal{O}_L/P\mathcal{O}_L$ are all different, but the image of Q_i^k is the same as the image of $Q_i^{e_i}$ for all $k \geq e_i$. That is, $Q_i^k + P\mathcal{O}_L = Q_i^{e_i}$ for all $k \geq e_i$. In $k[X]/(\overline{F}(X))$, the images of $(\overline{F}_i(X))^2, (\overline{F}_i(X))^2, \ldots, (\overline{F}_i(X))^{e_i}$ are all different, but all subsequent powers of e_i are the same as the image of $(\overline{F}_i(X))^{e_i}$.)

This completes the proof. □

As a corollary to this theorem, we can prove the fact stated earlier about the finiteness of ramified primes.

Theorem 5.3. *There are only finitely many prime ideals of $\mathcal{O}_K$ that ramify in $\mathcal{O}_L$.*

Proof. We apply Theorem 5.2 to $L = K(\theta)$, where $\theta \in \mathcal{O}_L$. Let P be relatively prime to the conductor I. It is enough to show that the reduction of F modulo P (denote it by $\overline{F}$) does not have any double roots (except for in finitely many cases), where F is the minimal polynomial of θ. Now, F has no double root if $\overline{F}$ and and its derivative $\overline{F}'$ are relatively prime. We know that F itself only has simpmle roots, so $(F, F') = 1$, hence we can find $G(X), H(X) \in K[X]$ such that $F(X)G(X) + F'(X)H(X) = 1$. We can multiply by a nonzero integer such that the coefficients will be algebraic integers to get $F(X)G^*(X) + F'(X)H^*(X) = m \neq 0$, where $G^*(X), H^*(X) \in \mathcal{O}_K[X]$. If we take P such that $m \notin P$, then $\overline{F}$ does not have multiple roots. Hence we can choose any prime ideal except for finitely many. This proves that indeed ramification is an exceptional case. □

In the special case when $K = \mathbb{Q}$, we can describe explicitly when a prime is ramified. The following theorem will be stated without proof as the proof is beyond the scope of this course.

Theorem 5.4. *Let L be a number field. A rational prime p is ramified in L if and only if p divides the discriminant of L.*

We have seen that if L has a complex embedding, then $|d_L| > 1$. (This was Exercise 5 of Problem Set 3.) But we in fact have something stronger than this.

Proposition 5.1. *If $L \neq \mathbb{Q}$, then $|d_L| > 1$.*

We now work the the case of cyclotomic fields explicitly. That is, we will now describe the decomposition of rational primes in a cyclotomic field.

Proposition 5.2. *Let $L = \mathbb{Q}(\zeta_n)$, where ζ_n is a primitive nth root of unity. Then in L we have the following decomposition: $p\mathcal{O}_L = (Q_1 \cdots Q_r)^{\varphi(p^{v_p})}$, where Q_i are distinct prime ideals with inertia degree f_p.*

Note that we in fact have enough information to determine r. We know $\varphi(n) = [L : \mathbb{Q}] = r f_p \varphi(p^{v_p})$, so $r = \frac{1}{f_p}\varphi(\frac{n}{p^{v_p}})$.

Remark. In the special case when n is a prime, we proved already that $\mathcal{O}_K = \mathbb{Z}[\zeta_n]$. We will prove later that this is true in general. For now, we assume this to be a fact and begin the proof of Proposition 5.2.

Proof. □

We now go on a slight tangent to make an interesting remark about zeta functions.

6. Application to Zeta Functions: 3 - 9 November 2010

If K is an algebraic number field, then we define the Dedekind zeta function to be $\zeta_K(s) := \sum_a (Na)^{-s}$, where $s \in \mathbb{C}$. If $\mathrm{Re}(s) > 1$, then it is absolutely convergent and $\lim_{x \in \infty} \frac{1}{x} |\{a \lhd \mathcal{O}_K : Na \leq x\}|$ is a nonzero number. (This number is related to the class number and also to the regulator.)

7. Hilbert's Ramification Theory: 10 - 17 November 2010

Let L/K be a Galois extension with $[L:K] =: n$, where L and K are algebraic number fields. Then $G := \mathrm{Gal}(L/K)$ acts on $\mathcal{O}_L$. If Q is a prime ideal of L lying above P (so $P = Q \cap K$), then σQ is a prime ideal of L lying above P, where $\sigma \in G$. (This is easy to see: $\sigma(Q \cap \mathcal{O}_K) = \sigma(Q) \cap \sigma(\mathcal{O}_K) = (\sigma Q) \cap \mathcal{O}_K = P$.) In fact, something stronger holds:

Proposition 7.1. *The prime ideals lying above a fixed prime ideal P are all (Galois) conjugates of each other. (That is, they are mapped onto each other by an element of G.)*

Proof. □

Let us now introduce some new terminology.

Definition 7.1. If Q is a prime ideal of L¡ we can consider the group

$$G_Q := \{\sigma \in G : \sigma Q = Q\} \leq G,$$

i.e. the set of $\sigma \in G$ that fix Q set-wise. We call G_Q the decomposition group of Q over K. By the Galois correspondence, we have a corresponding fixed field

$$Z_Q := \{x \in L : \sigma x = x \text{ for all } \sigma \in G_Q\}.$$

We call Z_Q the decomposition field of Q over K.

We have some properties about the decomposition group G_Q. We have $G_Q = \{1\} \Leftrightarrow Z_Q = L \Leftrightarrow P$ is totally split in L (it is the product of n distinct prime ideals). We have $G_Q = G \Leftrightarrow Z_Q = K \Leftrightarrow P$ is nonsplit (it only has 1 prime ideal factor).

Recall that we can write the prime decomposition $P\mathcal{O}_L = Q_1^{e_1} \cdots Q_r^{e_r}$, where the inertia degree of Q_i is denoted by f_i. Recall that we had a theorem that said $\sum_{i=1}^{r} e_i f_i = n$. By our above discussion, we see that if L/K is Galois, then $e_1 = \cdots = e_r =: e$ and $f_1 = \cdots = f_r =: f$. Hence the identity becomes, simply, $n = efr$, where $r = |G : G_Q|$. So we have $P\mathcal{O}_L = \left(\prod_\sigma \sigma Q\right)^e$, where σ runs over a set of representatives of the left cosets of G_Q in G.

The special case of abelian Galois extensions is very important in number theory. The Kronecker-Weber theorem states that if $L \supseteq \mathbb{Q}$ is an abelian extension, then L is contained in some $\mathbb{Q}(\zeta_n)$. This is a major result in class field theory, the theory of abelian extensions. There, they discuss things like Artin's L-functions, which is a generalization of Dirichlet L-functions.

Now we return to the theory.

Proposition 7.2. *Let $Q_Z = Q \cap Z_Q$ be the prime ideal of Z_Q below Q. Then*

i) Q_Z is nonsplit in L. (i.e. Q is the only prime lying above Q_Z.)
ii) Q over Z_Q has ramification index e and inertia degree f.
iii) The ramification index and the inertia degree of Q_Z over P are both 1.

Proof. □

From this new language we can in fact prove quadratic reciprocity in a different way. It arises as an easy corollary of the following proposition.

Proposition 7.3. *Let l and p be odd primes, $l \neq p$. Let ζ_l be a primitive lth root of unity. Then p is totally split in $\mathbb{Q}(\sqrt{l^*})$ where $l^* = \left(\frac{-1}{l}\right) l$ if and only if p splits in $\mathbb{Q}(\zeta_l)$ into an even number of prime ideals.*

Proof. □

Lemma 7.1. *If a is squarefree, p a prime, $(p, 2a) = 1$, then p is unramified in $\mathbb{Q}(\sqrt{a})$ and p is totally split in $\mathbb{Q}(\sqrt{d})$ if and only if $\left(\frac{a}{p}\right) = 1$.*

Proof. □

And now the following proposition (quadratic reciprocity) follows easily:

Proposition 7.4. *The following are equivalent:*

i) $\left(\frac{l^*}{p}\right) = 1$
ii) *p is totally split in $\mathbb{Q}(\sqrt{l^*})$*
iii) *p splits into an even number of prime ideals in $\mathbb{Q}(\zeta_l)$*
iv) *$\frac{l-1}{f_p}$ is even, where f_p is the smallest positive integers such that $p^{f_p} \equiv 1 \pmod{l}$.*

Proof. □

Returning to Hilbert ramification theory, we have a proposition regarding the construction of an integral basis.

Proposition 7.5. *Let $L/\mathbb{Q}$ and $L'/\mathbb{Q}$ be Galois extensions with relatively prime discriminant. Assume that their intersection if $\mathbb{Q}$. Then if $\omega_1, \ldots, \omega_n$ is an integral basis of L and $\omega_1', \ldots, \omega_n'$ is an integral basis of L', then the pairwise products form an integral basis of LL'. (Here, we have $n = [L : \mathbb{Q}]$ and $n' = [L' : \mathbb{Q}]$.*

Remark. Notice that the dimensions work out. That is, we know already that $[LL' : \mathbb{Q}] = nn'$, which is exactly the number of pairwise products.

Proof. □

Let L/K be a Galois extension and let Q be a prime ideal of $\mathcal{O}_L$. Let $G = \mathrm{Gal}(L/K), P = Q \cap K$, and let G_Q be the decomposition group of Q. If $\sigma \in G_Q$, the σ induces an automorphism $\overline{\sigma} : \mathcal{O}_L/Q \to \mathcal{O}_L/Q$, defined by $a \pmod{Q} \mapsto \sigma a \pmod{Q}$. Let $k = \mathcal{O}_K/P, l = \mathcal{O}_L/Q$. Then we get a homomorphism $G_Q \to \mathrm{Gal}(l/k)$. (Note here that l and k are finite fields and every extension of a finite field is Galois.) This is the identity on $\mathcal{O}_K/P$ since $\sigma|_K = \mathrm{id}_K$.

Proposition 7.6. *This homomorphism is surjective.*

8. p-adic Numbers and Hensel's Lemma: 30 November - 7 December 2010

In this last section of the course, we will discuss p-adic numbers and Hensel's lemma. This will cover just about the first four sections of Chapter II: The Theory of Valuations from Neukirch's book. (We will describe the p-adics in three different ways and prove the equivalences of each of these definitions.) Without further ado, we begin.

Let p be a rational prime. Then every integer $f > 0$ has a unique expansion

$$f = a_0 + a_1 p + \cdots + a_n p^n, 0 \leq a_i \leq p-1.$$

Extending this sum to an infinite sum, we get the notion of a p-adic integer.

Definition 8.1 (Definition 1)**.** Fix a prime $p > 0$. A *p-adic integer* is a formal sum

$$\sum_{i=1}^{\infty} a_i p^i = a_0 + a_1 p + \cdots + a_n p^n + \cdots, 0 \leq a_i \leq p-1.$$

The set of p-adic integers is denoted by $\mathbb{Z}_p$. Let

$$\mathbb{Z}_{(p)} := \{\frac{g}{h} : g, h \in \mathbb{Z}, p \nmid h\}.$$

If $\frac{g}{h} \in \mathbb{Z}_{(p)}$, then it has a unique expansion $\sum_{i=1}^{\infty} a_i p^i \in \mathbb{Z}_p$ such that $p^{n+1} \mid \left(\frac{g}{h} - \sum_{i=0}^{n} a_i p^i\right)$ for all $n \geq 0$.

From this, we define the p-adic numbers.

Definition 8.2 (Definition 1)**.** Define $\mathbb{Q}_p := \{\sum_{i=-m}^{\infty} a_i p^i, m \in \mathbb{Z}, 0 \leq a_i \leq p-1\}$. If $f \in \mathbb{Q}_p$, then we can write $f = \frac{g}{h} p^{-m}, (gh, p) = 1, m \in \mathbb{Z}$. If $a_0 + a_1 p + a_2 p^2 + \cdots + a_n p^n + \cdots$ is the expansion of $\frac{g}{h}$, then we call $a_0 p^{-m} + a_1 p^{-m+1} + \cdots + a_n p^{-m+n} + \cdots$ the *p-adic expansion of f.*

Remark. This is a unique expansion. If $f \in \mathbb{Q}$, we can give an element $\sum_{i=-m}^{\infty} a_i p^i \in \mathbb{Q}_p$ such that if $p^{e_n} \mid\mid f - \sum_{i=-m}^{n} a_i p^i$, then $e_n \to \infty$. In this way, we defined a map $\mathbb{Q} \to \mathbb{Q}_p$, which maps $\mathbb{Z}$ into $\mathbb{Z}_p$. (All we know now is that this is a set map, as we do not yet know the operational structure of $\mathbb{Q}_p$.) These maps are injective, so we can identify $\mathbb{Q}$ by its image in $\mathbb{Q}_p$, and hence we write $f = \sum_{i=-m}^{\infty} a_i p^i$.

We can also define the p-adics in a less element-oriented way. We consider the projective limit (also called the inverse limit).

Consider the sequence of projective maps

$$\mathbb{Z}/p\mathbb{Z} \xleftarrow{\lambda_1} \mathbb{Z}/p^2\mathbb{Z} \xleftarrow{\lambda_2} \mathbb{Z}/p^3\mathbb{Z} \xleftarrow{\lambda_3} \cdots.$$

From this, we get a projective limit:

$$\varprojlim_n \mathbb{Z}/p^n\mathbb{Z} := \{(x_n)_{x \geq 1} \in \prod_{n=1}^{\infty} \mathbb{Z}/p^n\mathbb{Z} : \lambda_n(x_{n+1}) = x_n, n = 1, 2, \dots\}.$$

It turns out that this is exactly the set of p-adic integers, and from the projective limit, we get Definition 2.

Proposition 8.1. *We define a map*

$$\varphi : \mathbb{Z}_p \to \varprojlim_n \mathbb{Z}/p^n\mathbb{Z}, \sum_{i=0}^{\infty} a_i p^i \mapsto (x_n)_{n \geq 1},$$

where $x_n = \sum_{i=0}^{n-1} a_i p^i$. This map is bijective.

By this proposition, we can consider $\mathbb{Z}_p$ as a ring, since the projective limit comes with a ring structure for free. Since every $f \in \mathbb{Q}_p$ has a representation $f = p^{-m} g, g \in \mathbb{Z}_p$, then we can define notions of division and multiplication on the set $\mathbb{Q}_p$. In this way, we see that $\mathbb{Q}_p$ is the field of fractions of $\mathbb{Z}_p$.

In the third definition, we approach the p-adics not from a series approach as in Definition 1, and also not an algebraic approach as in Definition 2, but from an analytic perspective. We

consider the p-adic exponential valuation of $\mathbb{Q}$ and look at the completion of the rationals under this valuation.

Definition 8.3 (Definition 3.)**.** (p-adic exponential valuation and the p-adic absolute value)

Consider the group of units in the ring of p-adic integers:

$$\mathbb{Z}_p^\times = \{x \in \mathbb{Z}_p : |x| = 1\}.$$

If we take any $x \in \mathbb{Q}_p^\times$ (the multiplicative group of p-adic numbers), we have $v_p(x) = m \in \mathbb{Z}$, so $v_p(xp^{-m}) = 0$, which means that xp^{-m} is a unit. Hence we can write any $x \in \mathbb{Q}_p^\times$ as $x = p^m \cdot \varepsilon$ where $m \in \mathbb{Z}$ and $\varepsilon \in \mathbb{Z}_p^\times$.

From this discussion arises the following proposition.

Proposition 8.2. *The nonzero ideals of $\mathbb{Z}_p$ are $p^n\mathbb{Z}_p = \{x \in \mathbb{Q}_p : v_p(x) \geq n\}, n \in \mathbb{Z}_{\geq 0}$ and $\mathbb{Z}_p/p^n\mathbb{Z}_p \cong \mathbb{Z}/p^n\mathbb{Z}$.*

Proof. Consider a nonzero ideal $I \lhd \mathbb{Z}_p$. Then let m be the minimal integer such that $x = p^m\varepsilon, \varepsilon \in \mathbb{Z}_p^\times$ for all nonzero $x \in I$. (Such an m exists since $I \leq \mathbb{Z}_p$ so $m \geq 0$. Then $I = p^m\mathbb{Z}_p$. (This m is in fact $v_p(x)$.)

We have a map $\varphi : \mathbb{Z} \to \mathbb{Z}_p/p^n\mathbb{Z}_p$ (since $\mathbb{Z} \subseteq \mathbb{Z}_p$). The kernel is clearly $p^n\mathbb{Z}$. In fact, $\ker\varphi = \mathbb{Z} \cap p^n\mathbb{Z}_p = \{x \in \mathbb{Z} : v_p(x) \geq n\} = p^n\mathbb{Z}$. It remains to be proven that φ is surjective. If $a \in \mathbb{Z}_p$, then there is an $x \in \mathbb{Z}$ such that $|x - a|_p \leq \frac{1}{p^n}$ (since $\mathbb{Z}$ is dense in $\mathbb{Z}_p$), which is equivalent to saying that $x - a \in p^n\mathbb{Z}_p$. Then $\varphi(x) = a \pmod{p^n\mathbb{Z}_p}$. This completes the proof. □

Now we prove the equivalence between Definition 2 and Definition 3. It is easy for this to become muddled in notation as our two different definitions use the same notation. Hence for the duration of this next proof, we will say that $\widetilde{\mathbb{Z}}_p$ is the p-adic numbers described in Definition 3. So we have, by the previous definition, $\widetilde{\mathbb{Z}}_p \to \widetilde{\mathbb{Z}}_p/p^n\widetilde{\mathbb{Z}}_p \cong \mathbb{Z}/p^n\mathbb{Z}$. In this way we can define a map

$$\varphi : \widetilde{\mathbb{Z}}_p \to \varprojlim_n \mathbb{Z}/p^n\mathbb{Z}.$$

Proposition 8.3. *This map is an isomorphism.*

Proof. If $x \in \widetilde{\mathbb{Z}}_p$ is mapped to 0, then $x \in p^n\mathbb{Z}_p$, so $v_p(x) \geq n$ for all n, so $x = 0$, which means that $\ker\varphi = \{0\}$. Now we want to show that this map is surjective.

We have seen that the elements of the projective limit are in a one-to-one correspondence with the formal sum $\sum_{i=0}^\infty a_i p^i$. Define a Caucy sequence $\{x_n\}$ as

$$x_n := \sum_{i=1}^n a_i p^i \in \mathbb{Z} \subseteq \widetilde{\mathbb{Z}}_p.$$

Since $\widetilde{\mathbb{Z}}_p$ is complete, then $\{x_n\}$ converges and we can let $x := \lim_{n\to\infty} x_n, x \in \widetilde{\mathbb{Z}}_p$. It can be checked that the image of x under φ is the given element of the projective limit and we are done. □

Definition 8.4. A *valuation* of a field K is a nonnegative function $|\cdot| : K \to \mathbb{R}$ such that

(i) $x \geq 0$ and $|x| = 0 \Leftrightarrow x = 0$.
(ii) $|xy| = |x||y|$
(iii) $|x + y| \leq |x| + |y|$. (If we have $|x + y| \leq \max(|x|, |y|)$, then we have a *"non-archimedian"* valuation.)

If $|\cdot|$ is a non-archimedean valuation, then $v(x) = -\log|x|$ for $x \neq 0$, $v(0) = \infty$. We also have the following properties:

(i) $v(x) = \infty \Leftrightarrow x = 0$
(ii) $v(xy) = v(x) + v(y)$
(iii) $v(x + y) \geq \min(v(x), v(y))$

This v is called the exponential valuation.

Consider $R = \{x \in K : v(x) \geq 0\} = \{x \in K : |x| \leq 1\}$. R is a ring and its group of units is $R^\times = \{x \in K, v(x) = 0\}$. And it has a unique maximal ideal $P = \{x \in K : v(x) > 0\}$. An exponential valuation is called *discrete* if $v(K^\times) = s\mathbb{Z}$ for some $s > 0$. It is *normalized* if $s = 1$. An element $a\pi \in R$ with $v(\pi) = 1$ is called a *prime element*. Every $x \in K^\times$ can be uniquely written as $x = \pi^m u$ for some $m \in \mathbb{Z}, u \in R^\times$.

Let K be a field, complete with respect to a non-archimedean discrete valuation $|\cdot|, R$ and P as above. Then a polynomial $f(X) = a_0 + a_1X + \cdots + a_nX^n \in R[X]$ is called *primitive* if $f(X) \not\equiv 0 \pmod P$, that is if $\max(|a_0|, |a_1|, \ldots, |a_n|) = 1$.

We now discuss Hensel's lemma.

Proposition 8.4 (Hensel's lemma)**.** *If a primitive polynomial $f(X) \in R[X]$ has a factorization $f(X) \cong \overline{g}(X)\overline{h}(X) \pmod P$ where $\overline{g}, \overline{h} \in k[X], (\overline{g}, \overline{h}) = 1$ in $k(X)$, then f has a factorization $f(X) = g(X)h(X)$ where $g, h \in R[X]$, $g \equiv \overline{g}, h \equiv \overline{h} \pmod P$ and $\deg g = \deg \overline{g}$.*

Corollary 8.1. *Let $f(X) = a_0 + a_1X + \cdot + a_nX^n \in K[X]$ be irreducible and $a_0a_n \neq 0$. Then $\max(|a_0|, |a_1|, \ldots, |a_n|) = \max(|a_0|, |a_n|)$. In particular, if $a_n = 1, a_0 \in R$, then $f(X) \in R[X]$.*

Theorem 8.1. *Let K be complete with respect to the discrete non-archimedean valuation $|\cdot|$ and let L/K be a finite extension. Then $|\cdot|$ can be uniquely extended to a valuation in L by the formula $|a| = \sqrt[n]{|N_{L/K}(a)|}$, where $a \in L, n = [L : K]$.*

Proposition 8.5. *Let k be an algebraic number field, let Q be a prime ideal of k, and for $x \in k\backslash\{0\}$, let $Q^{v_Q(x)} \,||\, (x)$. This is a discrete, exponential valuation of k, and $|x| = N(Q)^{-v_Q(x)}$. This is a discrete, non-archimedean valuation of k. Its completion is a finite extension of a p-adic field if Q lies above p.*