MATH 530 LECTURE NOTES

1. ALGEBRAIC NUMBERS AND ALGEBRAIC INTEGERS

A complex number is an algebraic integer (resp. algebraic number) if it is a root of some monic (leading coefficient 1) polynomial with coefficients in $\mathbb{Z}$ (resp. $\mathbb{Q}$). Notation: $\overline{\mathbb{Z}}, \overline{\mathbb{Q}}$.

A number field is a finite extension of $\mathbb{Q}$. Every number field takes the form $\mathbb{Q}(\alpha)$ for some algebraic number α (because every finite separable extension is simple), and if the degree of the minimal polynomial of α over $\mathbb{Q}$ is n, then $1, \alpha, \cdots, \alpha^{n-1}$ is a basis of $\mathbb{Q}(\alpha)$ as a v.s. over $\mathbb{Q}$.

Proposition 1.1. *Let α be an algebraic number. Then the minimal polynomial of α has integer coefficients if and only if α is an algebraic integer.*

Proof. $\Longrightarrow$ is obvious by definition. STP $\Longleftarrow$. Suppose α is an algebraic integer and let $f(x) \in \mathbb{Z}[x]$ be a monic integral polynomial having α as a root. Also let $g(x) \in \mathbb{Q}[x]$ be the (monic) minimal polynomial of α over $\mathbb{Q}$. Then $g(x)$ divides $f(x)$ and we may write $f(x) = g(x)h(x)$ for some $h(x) \in \mathbb{Q}[x]$. Want to show that $g(x)$ (and in fact also $h(x)$) has coefficients in $\mathbb{Z}$. Let m (resp. n) be the smallest natural number for which $mg(x)$ (resp. $nh(x)$) has integral coefficients. Then the coefficients of $mg(x)$ (resp. $nh(x)$) have no common factor. By Gauss's Lemma on polynomials, the coefficients of the product $mg(x) \cdot nh(x) = mn \cdot g(x)h(x)$ then have no common factor. As $g(x)h(x) \in \mathbb{Z}[x]$, this implies $mn = 1$, and so $m = n = 1$. □

What are the algebraic integers in a given number field? Some simple cases:

Corollary 1.2. *The only algebraic integers in $\mathbb{Q}$ are the ordinary integers.*

Corollary 1.3. *Let m be a square free integer. The set of algebraic integers in $\mathbb{Q}(\sqrt{m})$ is $\mathbb{Z}[\sqrt{m}] = \{a + b\sqrt{m}\}$ if $m \equiv 2, 3 \mod 4$, $\mathbb{Z}[\frac{1+\sqrt{m}}{2}] = \{\frac{a+b\sqrt{m}}{2} : a \equiv b \mod 2\}$ if $m \equiv 1 \mod 4$.*

Proof. Let $\alpha = r + s\sqrt{m}$ be an element in $\mathbb{Q}(\sqrt{m})$. If $s = 0$, then α is an algebraic integer iff $r \in \mathbb{Z}$. If $s \neq 0$, then the minimal polynomial of α is $x^2 - 2rx + r^2 - ms^2$. By the above prop, α is an algebraic integer iff both $2r$ and $r^2 - ms^2$ belong to $\mathbb{Z}$. The rest of the proof is then an elementary exercise. □

We want to show that the algebraic integers in any given number field form a ring. For this, we need

Theorem 1.4. *TFAE for $\alpha \in \mathbb{C}$.*

(1) α is an algebraic integer.

(2) The additive group of the ring $\mathbb{Z}[\alpha]$ is finitely generated.

(3) α is a member of some subring of $\mathbb{C}$ having a finitely generated additive group.

(4) $\alpha A \subset A$ for some finitely generated additive subgroup $A \subset \mathbb{C}$.

Proof. (1) $\implies$ (2): if α is a root of some monic polynomial over $\mathbb{Z}$ of degree n, then the additive group of $\mathbb{Z}[\alpha]$ is generated by $1, \alpha, \cdots, \alpha^{n-1}$. (2) $\implies$ (3) $\implies$ (4) are obvious. It remains to show (4) $\implies$ (1). Let $a_1, \cdots, a_n$ generate A. Expressing each αa_i as a $\mathbb{Z}$-linear combo of $a_1, \cdots, a_n$. We obtain

$$\begin{pmatrix} \alpha a_1 \\ \cdots \\ \alpha a_n \end{pmatrix} = M \begin{pmatrix} a_1 \\ \cdots \\ a_n \end{pmatrix}$$

where M is an n by n matrix over $\mathbb{Z}$. Equivalently,

$$(\alpha I - M) \begin{pmatrix} a_1 \\ \cdots \\ a_n \end{pmatrix} = \begin{pmatrix} 0 \\ \cdots \\ 0 \end{pmatrix}$$

As $a_1, \cdots, a_n$ are not all zero, this implies that $\det(\alpha I - M) = 0$. Expressing this det in term of the n^2 coordinates of $\alpha I - M$, we obtain a monic polynomial over $\mathbb{Z}$ having α as a root. □

Corollary 1.5. *If α and β are algebraic integers, so are their sum and product.*

Proof. We know that $\mathbb{Z}[\alpha]$ and $\mathbb{Z}[\beta]$ have finitely generated additive groups, then so does $\mathbb{Z}[\alpha, \beta]$. As $\alpha + \beta$ and $\alpha\beta$ belong to $\mathbb{Z}[\alpha, \beta]$, characterization (3) implies that they are algebraic integers. □

So the algebraic integers in any given number field form a ring, we call such kind of rings *number rings*. Notation: O_F denotes the ring of integers of F.

Remark 1.6. The above arguments generalize to the case when $\mathbb{Z}$ is replaced by an integral domain A and $\mathbb{C}$ is replaced by a field Ω containing A. See Milne, beginning of Chapter 2.

2. Cyclotomic fields and their Galois groups

The cyclotomic fields are the most fundamental examples of number fields. Let $n > 2$ be an integer and let $\omega = e^{\frac{2\pi i}{n}}$. We study the field $\mathbb{Q}(\omega)$ and determine its Galois group over $\mathbb{Q}$. Define

$$\Phi_n(x) = \prod_{1 \le k \le n, (k,n)=1} (x - \omega^k)$$

It is called the n-th cyclotomic polynomial. Notice that $x^n - 1 = \prod_{d|n} \Phi_d(x)$.

Exercise: show that $\Phi_n(x)$ is in $\mathbb{Z}[x]$.

We will show that $\Phi_n(x)$ is irreducible over $\mathbb{Q}$. For this, it is enough to show that $\omega \sim \omega^k$ for any k s.t. $(k, n) = 1$. This can be reduced to the following proposition:

Proposition 2.1. *Let θ be a root of $\Phi_n(x)$ and p be a prime not dividing n. Then $\theta \sim \theta^p$.*

Remark 2.2. Once we have the proposition, we can apply it repeatedly to obtain $\omega \sim \omega^k$ for any k prime to n.

Proof. Let $f(x)$ be the minimal polynomial of θ over $\mathbb{Q}$. We want to show that $f(\theta^p) = 0$. First, f divides Φ_n and we write

$$\Phi_n(x) = f(x)g(x)$$

for some $g(x) \in \mathbb{Q}[x]$. Since $\Phi_n(x)$ has integral coefficients, an argument using Gauss's Lemma shows that both f and g have integral coefficients. By definition of Φ_n, $\Phi_n(\theta^p) = 0$, so if θ^p is not a root of f, then $g(\theta^p) = 0$, i.e. θ is a root of $g(x^p)$. It follows (just like the above) that $f(x)$ divides $g(x^p)$ and we can write

$$g(x^p) = f(x)h(x)$$

for some $h(x) \in \mathbb{Z}[x]$. Reducing the coefficient modulo p and noticing that $g(x^p) \equiv g(x)^p \bmod p$, we see that $\bar{f}(x)$ divides $\bar{g}(x)^p$ in $\mathbb{F}_p[x]$. In particular, $\bar{f}$ and $\bar{g}$ have a common factor, say $\bar{k}$. Then $\bar{k}^2 | \bar{f}\bar{g} = \bar{\Phi}_n$. It follows that $\bar{\Phi}_n$ has repeated roots in $\overline{\mathbb{F}}_p$, and so $x^n - \bar{1}$ has repeated roots in $\overline{\mathbb{F}}_p$ (since the former divides the latter). On the other hand, the derivative of $x^n - \bar{1}$ is $\bar{n}x^{n-1}$, which is nonzero since p does not divide n by assumption. So $x^n - \bar{1}$ and $\bar{n}x^{n-1}$ are coprime in $\mathbb{F}_p[x]$, and hence $x^n - \bar{1}$ has no repeated root, a contradiction. □

Corollary 2.3. *$\Phi_n(x)$ is irreducible over $\mathbb{Q}$ and $[\mathbb{Q}(\omega) : \mathbb{Q}] = \varphi(n)$.*

Corollary 2.4. $\mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$.

Proof. Define a map from the latter to the former by sending $k \in (\mathbb{Z}/n\mathbb{Z})^\times$ to $\sigma_k \in \mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q})$ defined by $\sigma_k(\omega) = \omega^k$ (σ_k exists by the irreducibility of Φ_n). I leave the rest of the proof to you. □

3. Some algebra

Let K be a field and let Ω be an algebraically closed field containing K. Suppose L is a subfield of Ω such that L/K is a finite separable extension of degree n. Then L has exactly n K-embeddings into Ω. Here a K-embedding of L into Ω is a field homomorphism $\sigma : L \to \Omega$ that fixes K pointwisely. In fact, we have $L = K(\theta)$ for some $\theta \in L$, and θ has exactly n conjugates over K, and each conjugate uniquely determine a K-embedding of L into Ω. The same argument gives that every embedding of K into Ω extends to exactly n embeddings of L into Ω. Let M/K be a finite normal extension containing L, then every K-embedding of L in Ω extends to exactly $[M : L]$ K-embeddings of M in Ω, and since M/K is normal, each of such embeddings can be identified with an element of $\mathrm{Gal}(M/K)$.

In particular, if $K = \mathbb{Q}$, $\Omega = \mathbb{C}$ and $L = \mathbb{Q}(\theta)$ for some algebraic number θ of degree n, suppose r of the conjugates of θ are real and s pairs of the conjugates of θ are nonreal, then $r + 2s = n$ and r embeddings of L in $\mathbb{C}$ fall in $\mathbb{R}$ (real embedddings) and $2s$ embeddings of L in $\mathbb{C}$ do not fall in $\mathbb{R}$ (complex embeddings). Say L is totally real if all its embeddings in $\mathbb{C}$ are real. For example, $\mathbb{Q}(\sqrt[3]{2})$ has one real embedding and two complex embeddings in $\mathbb{C}$.

Now we come back to the general setting and let $\sigma_1, \cdots, \sigma_n$ be the distinct K-embeddings of L in Ω. For any $\alpha \in L$, define

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

and

$$\mathrm{N}_{L/K}(\alpha) = \sigma_1(\alpha) \cdots \sigma_n(\alpha).$$

It is easy to see that $\mathrm{Tr}_{L/K}(\alpha+\beta) = \mathrm{Tr}_{L/K}(\alpha)+\mathrm{Tr}_{L/K}(\beta)$ and $\mathrm{N}_{L/K}(\alpha\beta) = \mathrm{N}_{L/K}(\alpha)\,\mathrm{N}_{L/K}(\beta)$.

Proposition 3.1. *Let $r = [L : K(\alpha)]$ and let $\alpha = \alpha_1, \cdots, \alpha_k$ be the distinct conjugates of α over K. Then*

$$\mathrm{Tr}_{L/K}(\alpha) = r(\alpha_1 + \cdots + \alpha_k)$$

and

$$\mathrm{N}_{L/K}(\alpha) = (\alpha_1 \cdots \alpha_k)^r.$$

In particular, they belong to K, and if $\alpha \in \overline{\mathbb{Z}}$, then they belong to O_K.

Proof. Each α_i determines a unique K-embedding of $K(\alpha)$ in Ω, and each such embedding extends to exactly r K-embeddings of L in Ω. □

Proposition 3.2. $\mathrm{Tr}_{L/K}(\alpha) = \mathrm{Tr}\, m_\alpha$, $\mathrm{N}_{L/K}(\alpha) = \det m_\alpha$. *Here $m_\alpha : L \to L$ is the K-linear map induced by multiplication by α.*

Proof. First reduce to the case $L = K(\alpha)$, then compute the matrix of m_α with respect to the power basis $1, \alpha, \alpha^2, \cdots$. □

Proposition 3.3. *Suppose $K \subset L \subset M$. Then*

$$\mathrm{Tr}_{M/K} = \mathrm{Tr}_{L/K} \circ \mathrm{Tr}_{M/L}$$
$$\mathrm{N}_{M/K} = \mathrm{N}_{L/K} \circ \mathrm{N}_{M/L}$$

4. The discriminant

Let K be a number field of degree n over $\mathbb{Q}$. Let $\sigma_1, \cdots, \sigma_n$ denote the n embeddings of K in $\mathbb{C}$. For any n-tuple of elements $\alpha_1, \cdots, \alpha_n$ in K, define the discriminant of $\alpha_1, \cdots, \alpha_n$ to be

$$d(\alpha_1, \cdots, \alpha_n) = |\sigma_i(\alpha_j)|^2$$

i.e., the square of the determinant of the matrix having $\sigma_i(\alpha_j)$ in the ith row, jth column. (Notation: we will write $[a_{ij}]$ to denote the matrix having a_{ij} in the ith row, jth column, and $|a_{ij}|$ to denote its determinant.) Notice that the square makes the discriminant independent of the ordering of the σ_i and the ordering of the α_j.

Proposition 4.1.

$$d(\alpha_1, \cdots, \alpha_n) = |\,\mathrm{Tr}_{K/\mathbb{Q}}(\alpha_i\alpha_j)|$$

In particular, $d \in \mathbb{Q}$, and if all α_i are algebraic integers, then $d \in \mathbb{Z}$.

Proof.

$$[\sigma_j(\alpha_i)][\sigma_i(\alpha_j)] = [\sigma_1(\alpha_i\alpha_j) + \cdots + \sigma_n(\alpha_i\alpha_j)] = [\mathrm{Tr}_{K/\mathbb{Q}}(\alpha_i\alpha_j)]$$

Then take the det on both sides. □

Proposition 4.2. $d(\alpha_1, \cdots, \alpha_n) = 0$ *iff* $\alpha_1, \cdots, \alpha_n$ *are LD over* $\mathbb{Q}$.

Proof. $\Longleftarrow$: if $\sum a_j\alpha_j = 0$ for some $a_j \in \mathbb{Q}$ not all zero, then for any i, $\sum a_j\sigma_i(\alpha_j) = 0$, and hence the columns of the matrix $[\sigma_i(\alpha_j)]$ satisfies the same LD relation; so the det must be zero.

Conversely, if $d = 0$, then the rows R_i of $[\mathrm{Tr}_{K/\mathbb{Q}}(\alpha_i\alpha_j)]$ are LD, so $\sum a_iR_i = (0, \cdots, 0)$ for some rationals a_i not all zero. Considering only the jth coordinate of each row, we obtain $0 = \sum a_i \mathrm{Tr}_{K/\mathbb{Q}}(\alpha_i\alpha_j) = \mathrm{Tr}_{K/\mathbb{Q}}((\sum a_i\alpha_i)\alpha_j)$. Set $\alpha = \sum a_i\alpha_i$. If $\alpha_1, \cdots, \alpha_n$ are LI over $\mathbb{Q}$, then they form a basis of K over $\mathbb{Q}$, and $\alpha \neq 0$ since the a_i's are not all zero. It follows that $\alpha\alpha_1, \cdots, \alpha\alpha_n$ also form a basis of K over $\mathbb{Q}$. Since $\mathrm{Tr}_{K/\mathbb{Q}}$ is zero on the these vectors, it is zero on every element of K, which is absurd. □

In particular, every basis for K over $\mathbb{Q}$ has nonzero discriminant. How are the discriminants of different bases related?

Proposition 4.3. *Suppose $\alpha_1, \cdots, \alpha_n$ and $\beta_1, \cdots, \beta_n$ are bases for K over $\mathbb{Q}$. Write $\beta_j = \sum a_{ij}\alpha_i$ for rationals a_{ij}. Then $d(\beta_1, \cdots, \beta_n) = |a_{ij}|^2 d(\alpha_1, \cdots, \alpha_n)$.*

Proof. Easy exercise. □

Suppose $K = \mathbb{Q}(\alpha)$, then $1, \alpha, \cdots, \alpha^{n-1}$ is a basis of K as a v.s. over $\mathbb{Q}$ (called power basis). Let $f(x)$ be the minimal polynomial of α over $\mathbb{Q}$ with roots $\alpha_1, \cdots, \alpha_n$.

Proposition 4.4. $d(1, \alpha, \cdots, \alpha^{n-1}) = \prod_{i<j}(\alpha_i - \alpha_j)^2 = (-1)^{\frac{n(n-1)}{2}} \mathrm{N}_{K/\mathbb{Q}}(f'(\alpha))$.

Proof. □

So far we have been talking about the discriminant of an n-tuple of elements in K. Later we will define a notion of discriminant that only depends on the number field K.

5. Integral bases of a number field

This time we will show that for any number field K, O_K is a free abelian group of rank $[K : \mathbb{Q}]$. We begin with a fact on abelian groups:

Theorem 5.1. *If M is an abelian group generated by n elements and N is a subgroup of M, then N has a generating set consisting of at most n elements.*

Proof. Outlined in a HW exercise. □

Corollary 5.2. *If $N \subset M \subset N'$ are abelian groups such that N and N' are free of rank n, then M is free of rank n.*

Now suppose K is a number field of degree n over $\mathbb{Q}$. By the corollary, to show that O_K is a free abelian group of rank n, it is enough to show two things:

- O_K contains a free abelian group of rank n.
- O_K is contained in a free abelian group of rank n.

The first item is easy to show: first observe that if $\alpha \in \overline{\mathbb{Q}}$, then there is an integer d s.t. $d\alpha \in \overline{Z}$. So there exists a basis for K over $\mathbb{Q}$ consisting entirely of algebraic integers, which spans a rank-n free abelian subgroup of O_K.

For the second item, we need

Proposition 5.3. *Let $\alpha_1, \cdots, \alpha_n$ be a basis for K over $\mathbb{Q}$ consisting entirely of algebraic integers and set $d = d(\alpha_1, \cdots, \alpha_n)$. Then*

$$O_K \subset \mathbb{Z}(\alpha_1/d) + \cdots + \mathbb{Z}(\alpha_n/d).$$

Proof. Let $\alpha \in O_K$, we can write $\alpha = x_1\alpha_1 + \cdots + x_n\alpha_n$ for rationals x_i. Let $\sigma_1, \cdots, \sigma_n$ denote the n embeddings of K in $\mathbb{C}$. Applying σ_i to the above equation, we get $\sigma_i(\alpha) = x_1\sigma_i(\alpha_1) + \cdots + x_n\sigma_i(\alpha_n)$. Viewing this as a linear system with indeterminates $x_1, \cdots, x_n$ and applying Cramer's rule, we obtain $x_i = y_i/\delta$ where $\delta = |\sigma_i(\alpha_j)|$ and y_i is obtained from δ by replacing the ith row with the $\sigma_i(\alpha)$. Both y_i and δ are algebraic integers and $\delta^2 = d$. So $dx_i = \delta y_i$ is an algebraic integer; but since $dx_i \in \mathbb{Q}$, dx_i is an ordinary integer. Thus

$$\alpha = (dx_1)(\alpha_1/d) + \cdots + (dx_n)(\alpha_n/d) \in \mathbb{Z}(\alpha_1/d) + \cdots + \mathbb{Z}(\alpha_n/d).$$

□

Corollary 5.4. *O_K is a free abelian group of rank n.*

In other words, there exists $\beta_1, \cdots, \beta_n \in O_K$ such that every element of O_K can be uniquely represented as a $\mathbb{Z}$-linear combo of the β_i. Such an n-tuple of elements is called an *integral basis* for K over $\mathbb{Q}$. See Milne, Prop 2.29 for a more general argument, which implies the above corollary.

Now we define an important invariant of number fields.

Definition 5.5. Let K be a number field. We define the discriminant of K as follows:

$$d_K = d(\beta_1, \cdots, \beta_n)$$

where $\beta_1, \cdots, \beta_n$ is an integral basis of K. It is a nonzero integer.

It is easy to see that d_K is independent of the choice of an integral basis: If $\gamma_1, \cdots, \gamma_n$ is another integral basis, then $\begin{pmatrix} \gamma_1 \\ \cdots \\ \gamma_n \end{pmatrix} = M \begin{pmatrix} \beta_1 \\ \cdots \\ \beta_n \end{pmatrix}$ for some n by n matrix M over $\mathbb{Z}$. It follows that $d(\gamma_1, \cdots, \gamma_n) = |M|^2 d(\beta_1, \cdots \beta_n)$; in particular, $d(\gamma_1, \cdots, \gamma_n)$ and $d(\beta_1, \cdots \beta_n)$ have the same sign and $d(\beta_1, \cdots \beta_n) | d(\gamma_1, \cdots, \gamma_n)$. A similar argument shows $d(\gamma_1, \cdots, \gamma_n) | d(\beta_1, \cdots \beta_n)$. We conclude that the discriminants are equal.

It is also easy to see that if $\gamma_1, \cdots, \gamma_n \subset \overline{\mathbb{Z}}$ is a basis for K over $\mathbb{Q}$, then they form an integral basis iff $d(\gamma_1, \cdots, \gamma_n) = d_K$.

Example 5.6. Let m be a square free integer. If $m \equiv 2, 3 \mod 4$, then $1, \sqrt{m}$ is an integral basis for $\mathbb{Q}(\sqrt{m})$ and $d = 4m$; if $m \equiv 1 \mod 4$, then $1, \frac{1+\sqrt{m}}{2}$ is an integral basis for $\mathbb{Q}(\sqrt{m})$ and $d = m$.

6. Finding an integral basis

Let $K = \mathbb{Q}$ be a number field of degree n over $\mathbb{Q}$. We say K is monogenic if there is an algebraic integer α such that $1, \alpha, \cdots, \alpha^{n-1}$ is an integral basis for K. Such a basis is called a power basis. In this case, $O_K = \mathbb{Z}[\alpha]$. Not all number fields are monogenic: the first counterexample was found by Dedekind, who showed that $\mathbb{Q}(\theta)$ is not monogenic where θ satisfies $\theta^3 - \theta^2 - 2\theta - 8 = 0$.

Proposition 6.1. *Suppose that $K = \mathbb{Q}(\alpha)$ for an algebraic integer α of degree n over $\mathbb{Q}$, and $d(\alpha) := d(1, \alpha, \cdots, \alpha^{n-1})$ is a square free integer, then $O_K = \mathbb{Z}[\alpha]$.*

Proof. Let $\beta_1, \cdots, \beta_n$ be an integral basis. Let M be the transition matrix from this basis to the above power basis. So $d(\alpha) = |M|^2 d_K$. By assumption, $d(\alpha)$ is square free, $|M| = \pm 1$, and hence $d(\alpha) = d_K$. It follows that $1, \alpha, \cdots, \alpha^{n-1}$ is an integral basis. □

In practice, we can calculate $d(\alpha)$ by using the minimal polynomial of α, for example,

Example 6.2. If α is a root of $f(x) = x^n + ax + b$ for $a, b \in \mathbb{Z}$, then $d(\alpha) = (-1)^{n(n-1)/2} N_{K/\mathbb{Q}}(f'(\alpha))$, which equals $(-1)^{n(n-1)/2}(n^n b^{n-1} + (-1)^{n-1}(n-1)^{n-1} a^n)$.

Example 6.3. Let α be a root of the irrd poly $x^3 + x + 1$, then the ring of integers of $K = \mathbb{Q}(\alpha)$ equals $\mathbb{Z}[\alpha]$. In fact, $d(\alpha) = -31$, which is square free.

Next, we compute the ring of integers of cyclotomic fields.

Theorem 6.4. *Let p be an odd prime and $\omega = e^{2\pi i/p}$, then the ring of integers of $\mathbb{Q}(\omega)$ is $\mathbb{Z}[\omega]$.*

Lemma 6.5. $N_{\mathbb{Q}(\omega)/\mathbb{Q}}(1 - \omega) = \prod_{1 \le k \le p-1}(1 - \omega^k) = p$.

Proof. The minimal poly of ω is $x^{p-1} + \cdots + x + 1 = \prod_{1 \le k \le p-1}(x - \omega^k)$. Letting $x = 1$, we get $p = N_{\mathbb{Q}(\omega)/\mathbb{Q}}(1 - \omega)$. □

Lemma 6.6. $d(\omega) = d(1 - \omega) = (-1)^{(p-1)(p-2)/2} p^{p-2}$.

Proof. Homework exercise. □

Proof. (of the theorem) The degree of $\mathbb{Q}(\omega)$ is $p - 1$. Note that $\mathbb{Z}[\omega] = \mathbb{Z}[(1 - \omega)]$, and $1, 1 - \omega, \cdots, (1 - \omega)^{p-2}$ is a basis of $\mathbb{Q}(\omega)$ over $\mathbb{Q}$. By the lemma and a result we proved last time, O is contained in $\mathbb{Z}1 + \cdots + \mathbb{Z}(1 - \omega)^{p-2}/p^{p-2}$. We want to show that $O = \mathbb{Z}1 + \cdots + \mathbb{Z}(1 - \omega)^{p-2}$. Assume not, then there must be an element in O of the form

$$\frac{m_0 + m_1(1 - \omega) + \cdots + m_{p-2}(1 - \omega)^{p-2}}{p^{p-2}}$$

where $m_i \in \mathbb{Z}$ and not all m_i are divisible by p^{p-2}. For $m \in \mathbb{Z}$, let $v(m)$ be the integer for which $p^{v(m)}$ is the largest power of p dividing m. Let v denote the minimum of $v(m_0), \cdots, v(m_{p-2})$ $(v < p - 2)$ and let i be the smallest integer for which $v(m_i) = v$. Dividing the denom and the numer by p^v, get

$$\frac{m_0' + m_1'(1 - \omega) + \cdots + m_{p-2}'(1 - \omega)^{p-2}}{p^{p-2-v}}$$

where $m_i' \in \mathbb{Z}$ and $v(m_j') > 0$ for $j < i$, and $v(m_i') = 0$. The expression still belong to O when we replace the denom by p; and since p divides m_j for $j < i$,

$$\alpha := \frac{m_i'(1-\omega)^i + \cdots + m_{p-2}'(1-\omega)^{p-2}}{p}$$

belongs to O, where p does not divide m_i'. We have

$$p\alpha/(1-\omega)^{i+1} = m_i'/(1-\omega) + \text{algebraic integers}.$$

Since $1-\omega^k/1-\omega \in O$ and $i+1 \leq p-1$, the lemma implies that $p/(1-\omega)^{i+1} \in O$ and hence $p\alpha/(1-\omega)^{i+1} \in O$. It follows that $m_i'/(1-\omega) \in O$. So $p = N(1-\omega)|N(m_i') = m_i'^{p-1}$, a contradiction. □

A similar but more complicated argument shows that for $\omega = e^{2\pi i/p^n}$, the ring of integers of $\mathbb{Q}(\omega)$ is $\mathbb{Z}[\omega]$.

7. Some commutative algebra

Let A be an integral domain with fraction field K and let $S \in A - \{0\}$ be a multiplicative subset of A containing 1. We define the localization of A at S, denoted $S^{-1}A$, to be the subring $S^{-1}A := \{a/s : a \in A, s \in S\} \subset K$.

Exercise 7.1. (1) Let $\mathfrak{p}$ be a prime ideal of A such that $\mathfrak{p} \cap S = \phi$. Prove that $\mathfrak{p}(S^{-1}A)$ is a prime ideal of $S^{-1}A$.

(2) Prove that $\mathfrak{p} \mapsto \mathfrak{p}(S^{-1}A)$, $\mathfrak{q} \mapsto \mathfrak{q} \cap A$ are inverse bijections between the set of primes of A that don't intersect S and the set of prime ideals of $S^{-1}A$.

A commutative ring A is a local ring if it has a unique maximal ideal. This maximal ideal then necessarily consists of all the non-units of A.

Example 7.2. Let A be a integral domain and let $\mathfrak{p}$ be a prime ideal of A. Then $A_{\mathfrak{p}} := (A - \mathfrak{p})^{-1}A$ is a local ring with maximal ideal $\mathfrak{p}A_{\mathfrak{p}}$.

Definition 7.3. A d.v.r is a PID that has exactly one nonzero prime ideal.

Fact: A PID is a d.v.r iff it has exactly one prime element up to associates iff it is a local ring and is not a field.

Example 7.4. The ring $\mathbb{Z}_{(p)}$ is a d.v.r with (p) its unique prime ideal. units=? prime elements=?

Proposition 7.5. *Let A be a d.v.r. with fraction field K and let π be a prime element of A. Then every $x \in K^\times$ can be expressed uniquely in the form $x = u\pi^m$ with $m \in \mathbb{Z}$ and $u \in A^\times$. Define a (group) homom $v : K^\times \to \mathbb{Z}$ by $v(x) = m$. Then for all $x, y \in K^\times$, $v(x+y) \geq \min(v(x), v(y))$.*

Definition 7.6. Let K be a field. A discrete valuation on K is a homom $v : K^\times \to \mathbb{Z}$ such that $v(x+y) \geq \min(v(x), v(y))$.

We may extend v to K by letting $v(0) = \infty$. We say v is trivial if $v(x) = 0$ for all $x \in K^\times$.

Proposition 7.7. *Let v be a nontrivial d.v. on K, then $A := \{x \in K : v(x) \geq 0\}$ is a d.v.r. with prime ideal $\mathfrak{m} := \{x \in K : v(x) > 0\}$.*

Proof. Since v is nontrivial, we may assume that $v(K^\times) = \mathbb{Z}$. The properties $v(xy) = v(x) + v(y)$ and $v(x+y) \geq \min(v(x), v(y))$ imply that A is a ring and m is an ideal, which is maximal since $\{x \in K : v(x) = 0\}$ consists of units. A is a PID because if I is a nonzero ideal of A and if $0 \neq a \in I$ is an element for which $v(a)$ is the smallest postive elmt in $v(I)$, then $I = (a)$. Moreover, if I is prime, then $v(a) = 1$, and hence I is unique. □

So there is a 1-1 correspondence between d.v.rs and fields with discrete valuations.

Recall that a (commutative) ring A is noetherian if it satisfies one of the following equivalent conditions:

(1) every ideal is finitely generated.

(2) every ascending chain of ideals eventually becomes constant.

(3) every nonempty set S of ideals in A has a maximal element, i.e. there exists an ideal in S not properly contained in any other ideal in S.

Definition 7.8. Let $A \subset B$ be domains. An element $b \in B$ is said to be integral over A if there is a monic polynomial $f(x)$ with coefficients in A such that $f(b) = 0$. B is said to be integral over A if every element of B is integral over A. The ring A is said to be integrally closed if for any $\alpha \in K := Frac(A)$, α is integral over A $\implies$ $\alpha \in A$.

Example 7.9. Any UFD is integrally closed. $\mathbb{Z}[\sqrt{5}]$ is not integrally closed.

8. Dedekind domains

Definition 8.1. A Dedekind domain (d.d. in short) is an integral domain such that

- A is noetherian.
- A is integrally closed.
- every nonzero prime ideal is maximal.

Proposition 8.2. *Let A be a d.d. and S be a multiplicative subset of A. Then $S^{-1}A$ is a d.d.*

Proof. (1): we need to show that every ideal of $S^{-1}A$ is f.g. Let I be an ideal of $S^{-1}A$, then $I = S^{-1}(I \cap A)$ (check it). A is noetherian by assumption, so $I \cap A$ is finitely generated, and hence I is f.g. as well.

(2): **hw exercise**. A is i.c. implies that $S^{-1}A$ is i.c.

(3) follows immediately from the fact that there is a bijection between primes of A that don't intersect S and primes of $S^{-1}A$. □

Proposition 8.3. *Let A be a noetherian integral domain. Then A is a d.d. iff for every nonzero prime $\mathfrak{p}$, $A_\mathfrak{p}$ is a d.v.r.*

Proof. $\Longrightarrow$: hw exercise.

$\Longleftarrow$: A is noetherian by assumption. (This assumption is necessary bc there exists non-noetherian integral domains whose localization at every prime ideal is a d.v.r.) If there is a prime $\mathfrak{p}$ of A that is not maximal then there is a nonzero prime $\mathfrak{q}$ strictly containing $\mathfrak{p}$. It follows that $A_\mathfrak{q}$ has two nonzero primes: $\mathfrak{q}A_\mathfrak{q}$ and $\mathfrak{p}A_\mathfrak{q}$, contradicting to that $A_\mathfrak{q}$ is a d.v.r. It remains to show that A is i.c. Let $x \in K$ integral over A. and let I be the set of elements $a \in A$ such that $ax \in A$. For each nonzero $\mathfrak{p}$, x is integral over $A_\mathfrak{p}$ and hence $x \in A_\mathfrak{p}$ (since $A_\mathfrak{p}$ is i.c.). So there is $s \in A - \mathfrak{p}$ such that $sx \in A$, i.e. $s \in (A - \mathfrak{p}) \cap I$. It follows that for every $\mathfrak{p}$, I is not contained in $\mathfrak{p}$, and hence $I = A$. In particular, $1 \in I$, and hence $x \in A$. □

Now we prove

Theorem 8.4. *Let K be a number field with ring of integers O_K. Then O_K is a d.d.*

Proof. (1): Let I be an ideal. Since O_K is a f.g. abelian group and I is a subgroup, I is a f.g. $\mathbb{Z}$-module, *a fortiori* finitely generated as an ideal.

(2): An exercise in HW 1 shows that if α is the root of a monic polynomial whose coefficients are algebraic integers, then α is an algebraic integer.

(3): Let $\mathfrak{p}$ be a prime ideal of O, we need to show that $\mathfrak{p}$ is maximal, i.e. $O/\mathfrak{p}$ is a field. $\mathfrak{p} \cap \mathbb{Z}$ is either trivial or (p) for some prime number p. It can't be trivial: if we take a nonzero element $\beta \in \mathfrak{p}$, then there is an equation $\beta^n + a_1\beta^{n-1} + \cdots + a_n = 0$ for integers a_i. WMA $a_n \neq 0$. Then $a_n \in \beta O \cap \mathbb{Z} \subset \mathfrak{p} \cap \mathbb{Z}$. So $\mathfrak{p} \cap \mathbb{Z} = (p)$ for some prime number p. It follows that there is a canonical injection $\mathbb{Z}/p \to O/\mathfrak{p}$. Since O is integral over $\mathbb{Z}$, $O/\mathfrak{p}$ is algebraic over $\mathbb{Z}/p$. The following exercise will finish the proof. □

Exercise 8.5. (see HW 3) A integral domain containing a field k and is algebraic over k is itself a field.

Read the more general fact, Milne, Thm 3.29, which will be used later on.

9. Unique factorization in Dedekind domains

Our goal today is

Theorem 9.1. *Every ideal in a d.d. A is uniquely representable as a product of prime ideals.*

Since the ring of integers in a number field is a d.d., we have

Corollary 9.2. *For any number field K, every ideal O_K is uniquely representable as a product of prime ideals.*

A key input to its proof is the following

Theorem 9.3. *If I is an ideal in a d.d. A. Then there is an ideal J s.t. IJ is principal.*

We will first explain how the above theorem implies unique factorization in d.d., and then prove it.

Corollary 9.4. *If I_1, I_2, I_3 are ideals in a d.d. A, and $I_1I_2 = I_1I_3$, then $I_2 = I_3$.*

Proof. There is an ideal J s.t. $JI_1 = (a)$ for some $a \in A$; then $aI_2 = aI_3$, so $I_2 = I_3$. □

Corollary 9.5. *If I, J are ideals in a d.d. A, then $I|J$ iff $I \supset J$.*

Proof. $\Longrightarrow$: let $J = II'$, then $J \subset I$. $\Longleftarrow$: suppose $J \subset I$, fix I' s.t. $II' = (a)$ for some $a \in A$. Consider $J' := \frac{1}{a}I'J$, which is contained in $\frac{1}{a}I'I = \frac{1}{a}(a) = A$, and hence it is an ideal in A. It is clear that $IJ' = J$. □

Proof. (of unique factorization)

Existence: : If not, then the set of (proper) ideals which are not representable is nonempty and consequently has a maximal member M (since A is noetherian). It follows that M is contained in a maximal ideal P. Then $M = PI$ for some ideal I. Then I contains M. If $I = M$, then $P = A$ by the cancellation law, a contradiction; so I strictly contains M. By maximality of M, I is representable as a product of primes, and hence $M = PI$ is representable, contrary to assumption.

Uniqueness: Suppose $P_1...P_r = Q_1...Q_s$ where P_i and Q_i are primes, not necessarily distinct. Then $P_1 \supset Q_1...Q_s$. It follows that $P_1 \supset Q_i$ for some i (if not, then for every i there is $a_i \in Q_i - P_1$. It follows that $a_1...a_s \in Q_1...Q_s - P_1$ since P_1 is prime, a contradiction). WMA $P_1 \supset Q_1$. But both are maximal ideals (since A is a d.d.), we must have $P_1 = Q_1$. The cancellation law then implies that $P_2...P_r = Q_2...Q_s$. We can then finish by induction. □

It remains to prove 10.3. For this, we need two lemmas.

Lemma 9.6. *In a Dedekind domain, every ideal contains a product of prime ideals.*

Proof. Suppose not; then the set of ideals which do not contain such products is nonempty, and consequently has a maximal member M by noetherianity. M is certainly not a prime, so there exist $r, s \notin M$ s.t. $rs \in M$. Consider $M + (r)$ and $M + (s)$; both strictly contain M, so they both contain a product of primes by maximality of M. It follows that $(M+(r))(M+(s))$ contains a product of primes. But it is contained in M, so M contains a product of primes, contrary to assumption. □

Lemma 9.7. *Let I be a proper ideal in a d.d. A with field of fractions K. Then there is an element $c \in K - A$ s.t. $cI \subset A$.*

10. Unique factorization continued

Proof. Fix a nonzero element $a \in I$. By the previous lemma, $(a) \supset P_1...P_r$ for primes P_i. WMA r is minimized. So there exists $b \in P_2...P_r - (a)$. Then $c := b/a \in K - A$. On the other hand, I is contained in some maximal ideal P. So $P \supset P_1...P_r$. It follows that $P \supset P_i$ for some i. WMA $P \supset P_1$, so $P = P_1$ since A is a d.d. So

$$cI = \frac{1}{a}bI \subset \frac{1}{a}IP_2...P_r \subset \frac{1}{a}P_1P_2...P_r \subset \frac{1}{a}(a) = A.$$

□

Now we can prove 10.3, which will finish the proof of unique factorization in d.d.

Proof. Let a be a nonzero member of I and let $J = \{b \in A : bI \subset (a)\}$. Then $IJ \subset (a)$. Consider $L := \frac{1}{a}IJ$. It is an ideal contained in A. If $L \neq A$, then there is $c \in K - A$ s.t. $cL \subset A$ by lemma. $a \in I \implies J \subset L$. So $cJ \subset cL \subset A$. It follows that $(cJ) \cdot I = caL = a(cL) \subset aA = (a)$, and hence $cJ \subset J$ by definition of J.

J is finitely generated as an ideal, let $a_1, ..., a_m$ be a generating set. Then

$$c \begin{pmatrix} a_1 \\ ... \\ a_m \end{pmatrix} = M \begin{pmatrix} a_1 \\ ... \\ a_m \end{pmatrix}$$

for some matrix M over A. It follows that $\det(cI_m - M) = 0$. So $c \in K - A$ is integral over A, contradicting to that A is integrally closed.

This shows that $L = A$, i.e. $IJ = (a)$. □

Now we discuss some corollaries of unique factorization.

A very pleasant fact on d.d. is that divisibility among nonzero ideals is the same as containment: $I|J \iff I \supset J$. Suppose I and J are nonzero ideals in A, define $gcd(I, J)$ to be the greatest common ideal divisor, and define $lcm(I, J)$ to be the least commom ideal multiple. It follows that

$$gcd(I, J) = I + J$$
$$lcm(I, J) = I \cap J$$

If $I = P_1^{e_1}...P_n^{e_n}$ and $J = P_1^{f_1}...P_n^{f_n}$, then

$$gcd(I, J) = P_1^{min(e_1,f_1)}...P_n^{min(e_n,f_n)}$$
$$lcm(I, J) = P_1^{max(e_1,f_1)}...P_n^{max(e_n,f_n)}$$

It follows that

$$gcd(I, J)lcm(I, J) = IJ.$$

We say I and J are relatively prime (or coprime) if $I + J = (1)$. Note that I and J are coprime iff $I \cap J = IJ$ (which holds for in any commutative ring). The Chinese Remainder Theorem says that if $I_1, \cdots, I_n$ are pairwisely coprime ideals in a commutative ring A, then

$$A/I_1 \cdots I_n \cong \prod_{i=1}^{n} A/I_i$$

Proposition 10.1. *Let $P_1, ..., P_n$ be distinct prime ideals of A and let $e_1, ..., e_n$ be nonnegative integers. Then there is $a \in A$ s.t. for all i, (a) is divisible by $P_i^{e_i}$ but not $P_i^{e_i+1}$.*

Proof. Choose $a_i \in P_i^{e_i} - P_i^{e_i+1}$. By CRT, the system of equations

$$x \equiv a_i \mod P_i^{e_i+1}$$

has a solution. Let a be a solution, then $(a) \subset P_i^{e_i}$ and is not contained in $P_i^{e_i+1}$. So (a) is divisible by $P_i^{e_i}$ but not $P_i^{e_i+1}$. □

However, we have no control over which other prime ideals may occur in (a).

Theorem 10.2. *Let $I \supset J$ be nonzero proper ideals in A, then there is $a \in A$ such that $I = J + (a)$.*

Proof. $I = P_1^{e_1}...P_n^{e_n}$ and $J = P_1^{f_1}...P_n^{f_n}$. Since $I \supset J$, $I|J$ and hence $e_i \leq f_i$. The above prop gives an element a such that

$$(a) = P_1^{e_1}...P_n^{e_n}B$$

for some ideal B relatively prime to P_i for all i. Since $e_i \leq f_i$, it then follows that $gcd((a), J) = P_1^{e_1}...P_n^{e_n} = I$, i.e. $(a) + J = I$. □

Corollary 10.3. *Any nonzero ideal in a d.d. is generated by at most two elements.*

Exercise 10.4. Let A be an integral domain with only finitely many prime ideals; then A is a Dedekind domain if and only if it is a principal ideal domain.

Exercise 10.5. A Dedekind domain that is a unique factorization domain is a principal ideal domain.

(In general, a UFD is not necessarily a PID, e.g. $k[x, y]$ is a UFD yet it is neither a PID nor a d.d.)

Remark 10.6. Since the ring of integers of a number field is a d.d. All the results we have proved apply to them.

11. Interlude: Ideal class group

Let A be a d.d. with fraction field K. A fractional ideal of A is a nonzero A-submodule I of K for some nonzero $a \in A$, $aI \subset A$. Fractional ideals are *not* ideals unless they are contained in A. To avoid confusion, we will address ideals of A as *integral ideals* when necessary. For every $b \in K$, $(b) := bA$ is a fractional ideal, which is called *principal*. We can define the product of two fractional ideals I and J in the obvious way:

$$I \cdot J := \{\sum x_i y_i : x_i \in I, y_i \in J\}$$

which is also a fractional ideal.

Proposition 11.1. *The set $Id(A)$ of fractional ideals of a d.d. A forms a group.*

Proof. That every element has an inverse follows from the fact that for every integral ideal I, there is an integral ideal J s.t. IJ is principal. □

Proposition 11.2. *Let S be a multiplicative subset of a d.d. A. Then $I \mapsto S^{-1}I$ defines an isomorphism from the subgroup of $Id(A)$ generated by prime ideals not meeting S to the group $Id(S^{-1}A)$. (Recall that $S^{-1}A$ is again a d.d.)*

Proof. This follows immediately from the previous prop and the correspondence between primes of A and primes of $S^{-1}A$. □

Definition 11.3. The ideal class group $Cl(A)$ is defined to be the quotient

$$Cl(A) := Id(A)/P(A)$$

of $Id(A)$ by the subgroup of principal (fractional) ideals.

Remark 11.4. Later we will prove that for any number field K, $Cl(O_K)$ is finite. Its order $h_K := |Cl(O_K)|$ is called the *class number* of the field K. Understanding how the class numbers of number fields vary remains an interesting problem.

12. Decomposition of prime ideals in extensions

Let L/K be a finte extension of number fields. Let $A = O_K$ and $B = O_L$. A prime ideal P of A will factor in B:

$$PB = Q_1^{e_1}...Q_g^{e_g}$$

for distinct prime ideals Q_i in B (by the following lemma, PB is proper, and hence $g \geq 1$).

Lemma 12.1. *$PB \neq B$.*

Proof. By a fact we proved earlier (Lemma 9.7), there is an element $\gamma \in K - A$ such that $\gamma P \subset A$. Suppose $PB = B$, then $1 \in PB$, and hence $\gamma \in \gamma PB \subset AB = B$. It follows that $\gamma \in B \cap K = A$, a contradiction. □

If at least one of the e_i is greater than 1 then we say P is ramified in B (or L). Otherwise we say P is unramified in B (or L). If Q occurs in the decomposition of PB, we say Q divides P and write $e(Q|P)$ for the ramification index and $f(Q|P)$ for $[B/Q : A/P]$ (called the residue class degree; note that A/P and B/Q are finite fields of characteristic p, where $(p) = P \cap \mathbb{Z}$). Suppose that P is unramified in L, i.e. $e(Q_i|P) = 1$ for all i. P is said to be split (or split completely) in L if $f(Q_i|P) = 1$ for all i, and it is said to be inert in L if $g = 1$, i.e. PB remains to be a prime in B.

Lemma 12.2. *A prime ideal Q of B divides P iff $P = Q \cap K$.*

Proof. Recall that $Q|P$ iff $PB \subset Q$. $\implies$: Suppose $Q|P$, then $P \subset Q \cap K$, which cannot be A since Q is a proper ideal. Since P is maximal, we must have $P = Q \cap K$. $\impliedby$: Suppose $P = Q \cap K$, then $PB \subset Q$, which implies that $Q|P$. □

Theorem 12.3. *Let $n = [L : K]$ and let $Q_1, ..., Q_g$ be the prime ideals of B dividing P with ramification indices e_i and residue class degrees f_i; then $\sum_{i=1}^{g} e_i f_i = n$.*

Exercise 12.4. Let A be an integral domain with field of fractions K. Let L/K be a finite extension of fields and let B be the integral closure of A in L, i.e. B is the ring of all elements in L that are integral over A. Let S be a multiplicative subset of A. Show that $S^{-1}B$ is the integral closure of $S^{-1}A$ in L.

Proof. (of the theorem) We will show that both sides equal $[B/PB : A/P]$. First we show $\sum_{i=1}^{g} e_i f_i = [B/PB : A/P]$. CRT implies that $B/PB = \prod B/Q_i^{e_i}$. STP $[B/Q_i^{e_i} : A/P] = e_i f_i$. Consider the ideal chain

$$B \supset Q_i \supset Q_i^2 \supset .... \supset Q_i^{e_i}.$$

Observe that $Q_i^r/Q_i^{r+1} \cong B/Q_i$ as B/Q_i-vector spaces (**Exercise**: Take $c \in Q^r - Q^{r+1}$ and define a B/Q-linear map $\phi : B/Q \to Q^r/Q^{r+1}$ by $\phi(b + Q) = bc + Q^{r+1}$, show that ϕ is an isom). Hence it has dimension f_i as an A/P-vector space. Thus each quotient in the chain has dimension f_i over A/P, and hence $[B/Q_i^{e_i} : A/P] = e_i f_i$.

Second we show $[B/PB : A/P] = n$. Let $S = A - P$, $A' = S^{-1}A$ and $B' = S^{-1}B$. Then A' and B' are d.d., and B' is the integral closure of A' in L by the above exercise. Note that PA' is a prime ideal in A', and Q_iB' is a prime in B' (b/c $Q_i \cap S$ is empty). We have

$$PB' = (Q_1B')^{e_1} \cdots (Q_gB')^{e_g}$$

and

$$B'/Q_iB' \cong B/Q_i$$

(for the second one, see this week's homework set) Thus, $e(Q_iB'|PA') = e(Q_i|P) = e_i$ and $f(Q_iB'|PA') = f(Q_i|P) = f_i$. By the argument above, $\sum e(Q_iB'|PA')f(Q_iB'|PA') = [B'/PB' : A'/PA']$. So $[B/PB : A/P] = [B'/PB' : A'/PA']$. Thus, STP $[B'/PB' : A'/PA'] = n$. Note that A' is a PID by an exercise in HW 3 (note that A isn't a PID in general. This is the reason why we took localizations). **Claim**: $B' \cong A'^n$ as A'-modules. Granted the claim, we get $B'/PB' \cong (A'/PA')^n$ by reducing modulo P, which shows that $[B'/PB' : A'/PA'] = n$. It remains to prove the claim. We first show that B' is free over A': By the main theorem of modules over PID, it is enough to show that B', as an A'-module, is finitely generated and torsion-free. Since B' is an integral domain, torsion-freeness is automatic. On the other hand, $B = O_L$ is finitely generated as a $\mathbb{Z}$-module, a fortiori as an A-module; it follows that B' is finitely generated as an A'-module. Thus, $B' \cong A'^m$ for some natural number m. Tensoring over K on both sides, we get $L \cong K^m$ and hence $m = n$. □

Corollary 12.5. *If L is Galois over K, then all the ramification numbers are equal, and all the residue class degrees are equal, and so $efg = n$.*

Proof. Let σ be an element in $\mathrm{Gal}(L/K)$, then σ induces an automorphism of B. It follows that if Q is a prime of B, so is σQ. Note that σ induces an isomorphism of A/P-vector spaces $B/Q \cong B/\sigma Q$, which implies that $f(Q|P) = f(\sigma Q|P)$. On the other hand, applying σ to $PB = Q_1^{e_1}...Q_g^{e_g}$ we get $PB = (\sigma Q_1)^{e_1}...(\sigma Q_g)^{e_g}$, which shows $e(Q|P) = e(\sigma Q|P)$ for all Q above P. Thus, it suffices to show that the action of Galois is transitive on the primes above P. Assume not, there there are primes Q and R above P s.t. R is not any of σQ for $\sigma \in \mathrm{Gal}(L/K)$. By CRT, we can find an element $b \in B$ s.t. $b \in R$ and $b \notin \sigma Q$ for all σ. Consider $N_{L/K}(b) := \prod \sigma(b)$. It is an element in A. On the one hand, $b \in R$, so $N_{L/K}(b) \in R \cap A = P$. On the other hand, $\sigma(b) \notin Q$ since $b \notin \sigma^{-1}Q$ by our choice of b; but $\prod \sigma(b) \in P \subset Q$, contradicting to that Q is a prime ideal. □

13. Computing prime factorizations

Theorem 13.1. *Let K be a number field. Suppose that there is a $\theta \in K$ such that $O_K = \mathbb{Z}[\theta]$, i.e. K is monogenic. Let $m(x)$ be the minimal poly of θ over $\mathbb{Z}$. Let p be a rational prime, and suppose*

$$m(x) \equiv m_1(x)^{e_1}...m_g(x)^{e_g} \mod p$$

where each $m_i(x)$ is irred over $\mathbb{F}_p$. Then

$$pO_K = P_1^{e_1}...P_g^{e_g}$$

where $P_i := (p, m_i(\theta))$ are prime ideals with $f_i := [O_K/P_i : \mathbb{Z}/p] = \deg m_i$.

Proof. First we show that P_i are prime ideals with $f_i = \deg m_i$. In fact,

$$O_K/P_i = \mathbb{Z}[\theta]/(p, m_i(\theta)) = \mathbb{Z}[x]/(p, m(x), m_i(x)) = \mathbb{F}_p[x]/(m_i(x))$$

is a field by irrd of $m_i(x)$ over $\mathbb{F}_p$. Also, $P_i + P_j = O_K$ for $i \neq j$. In fact, it suffices to check this modulo p. Since m_i and m_j are relatively prime in $\mathbb{F}_p[x]$, there are $s, t \in \mathbb{F}_p[x]$ s.t. $sm_i + tm_j = 1$. In particular, $s(\theta)m_i(\theta) + t(\theta)m_j(\theta) = 1$ in O_K/p, and hence $(m_i(\theta)) + (m_j(\theta)) = O_K/p$.

Next, note that $P_i^{e_i} \subset pO_K + (m_i(\theta)^{e_i})$ and $m_1(\theta)^{e_1}...m_g(\theta)^{e_g} \equiv m(\theta) = 0 \mod p$; it follows that $P_1^{e_1}...P_g^{e_g} \subset pO_K$, ie, pO_K divides $P_1^{e_1}...P_g^{e_g}$. Write $pO_K = P_1^{e_1'}...P_g^{e_g'}$, then $e_i \geq e_i'$. The standard formula gives $[K : \mathbb{Q}] = \sum e_i' f_i$. On the other hand, $[K : \mathbb{Q}] = \deg m = \sum e_i f_i$ by counting the degrees of the polynomials. This forces $e_i = e_i'$. The theorem is now proved. □

In case when K is not monogenic, the theorem still holds for all but finitely many primes:

Exercise 13.2. Take $\theta \in K$ such that $[O_K : \mathbb{Z}[\theta]]$ is finite. Prove that the theorem holds for primes p not dividing this index. (Hint: Observe that $O_K \equiv \mathbb{Z}[\theta] \mod p$.)

14. Ramification and discriminant

We follow Conrad's notes: `https://kconrad.math.uconn.edu/blurbs/gradnumthy/disc.pdf`

15. Minkowski's constant and finiteness of the class group

16. Dirichlet Unit Theorem

17. Non-archimedean abs values

A non-archimedean abs val on a field K is a function $|.| : K \to \mathbb{R}$ satisfying

- $|x| > 0$ except that $|0| = 0$.
- $|xy| = |x||y|$.
- $|x + y| \leq \max(|x|, |y|)$.

The third condition is known as the nonarchimedean or strong triangle inequality. One can show that it is equivalent to the condition that $\{1, 2, 3, \cdots\} \subset K$ is bounded w.r.t. $|.|$.

There is an obvious non-archimedean abs val on K, the trivial abs val: $|0| = 0$ and $|x| = 1$ for all $x \neq 0$. In what follows, all abs values are assumed to be nontrivial.

Example 17.1. Let K be a number field and P be a prime ideal. For any nonzero $a \in K$, let $v_P(a)$ be the exponent of P in the prime decomposition of the fractional ideal (a); and set $v_P(0) = \infty$. Then v_P is additive and $v_P(x + y) \geq \min(v_P(x), v_P(y))$ (so v_P is a discrete valuation on K). Define $|a|_P = N(P)^{-v_P(a)}$, it follows that $||_P$ is a non-archimedean abs val, called the normalized P-adic abs val.

There is a bijection between valuations on K and nonarchimedean absolute values on K: recall that $v : K \to \mathbb{R} \cup \infty$ is a valuation if $v(0) = \infty$, $v(xy) = v(x) + v(y)$ and $v(x + y) \geq \min(v(x), v(y))$ for all $x, y \in K$. For any such v, pick any positive real $e > 1$ and define $|x| = e^{-v(x)}$, then $|.|$ is a nonarchimedean abs val on K. Conversely, if $|.| : K \to \mathbb{R}_{\geq 0}$ is a nonarchimedean abs val on K, define $v : K \to \mathbb{R} \cup \infty$ by $v(x) = -\log |x|$, then v is a valuation on K. We will freely exchange the use of valuations and discrete abs vals in view of this bijection.

We say $|.|$ is discrete if $|K^\times|$ is a discrete subgroup of $\mathbb{R}_{>0}$, equivalently, $v(K^\times)$ is a lattice in $\mathbb{R}$.

Example 17.2. Let $|.|_p$ be the standard (normalized) p-adic abs value on $\mathbb{Q}$. Then $|\mathbb{Q}^\times|_p = \{p^n : n \in \mathbb{Z}\}$.

Exercise 17.3. Suppose $|.|$ is nonarchimedean. If $|x| \neq |y|$, show that $|x+y| = \max(|x|, |y|)$.

Proposition 17.4. *Let $|.|$ be a non-arch abs val on K and let v denote the corresponding valuation. Then*

- $A := \{a \in K : |a| \leq 1\} = \{a \in K : v(a) \geq 0\}$ *is a subring of K with*
- $U := \{a \in K : |a| = 1\} = \{a \in K : v(a) = 0\}$ *its group of units and*
- $m := \{a \in K : |a| < 1\} = \{a \in K : v(a) > 0\}$ *as its unique max ideal.*

$|.|$ is discrete iff m is principal, in which case A is a d.v.r.

Proof. The first assertion follows immediately from the strong triangle ineq. If the val is discrete, let $v := -\log ||$, then A is a d.v.r. with $m = \{a \in K : v(a) > 0\}$ generated by the element π for which $v(\pi)$ is the smallest positive element in $v(K^\times)$. Conversely, if $m = (\pi)$, then $|K^\times|$ is the subgroup of $\mathbb{R}_{>0}$ generated by $|\pi|$. □

Definition 17.5. A is called the valuation ring of K, m is called the maximal ideal of K, and $k := A/m$ is called the residue field of K.

Example 17.6. Let $K = \mathbb{Q}$ with the standard p-adic norm $|.|_p$, then $A = \mathbb{Z}_{(p)} := \{a/b \in \mathbb{Q} : \text{(a,b)=1 and b is not divisible by p}\}$, $m = p\mathbb{Z}_{(p)}$ and $k \cong \mathbb{F}_p$.

Note that $||$ defines a metric $d(x, y) := |x - y|$ on K, and hence a topology on K. When K is a number field and P is a prime, the topology induced by $||_P$ is called the P-adic topology on K.

Example 17.7. When $K = \mathbb{Q}$ and $|.| = |.|_p$, the open balls (which are also closed since $|.|_p$ is discrete) are $a + p^n\mathbb{Z}_{(p)}$ for $a \in \mathbb{Q}$ and $n \in \mathbb{Z}$.

How do we compare different abs vals?

Proposition 17.8. *Let $||_1$, $||_2$ be abs vals on K. with $||_1$ nontrivial. TFAE:*

- $||_1$ *and* $||_2$ *define the same topology on K.*
- $|a|_1 < 1$ *iff* $|a|_2 < 1$.
- $||_2 = ||_1^r$ *for some* $r > 0$.

Two abs vals are said to be equivalent if they satisfy any of the above conditions.

Proof. 1 $\implies$ 2: As $|a^n| = |a|^n$, $a^n \to 0$ w.r.t $||$ iff $|a| < 1$. Now if $|a|_1 < 1$, then $a^n \to 0$ w.r.t. $||_1$; so $a^n \to 0$ w.r.t. $||_2$ by assumption, and hence $|a|_2 < 1$.

2 $\implies$ 3: As $||_1$ is nontrivial, there exists $y \in K$ such that $|y|_1 > 1$. Then $|y|_2 > 1$ by assumption. Let $r \in \mathbb{R}$ be such that $|y|_2 = |y|_1^r$, then $r = \log|y|_2/\log|y|_1 > 0$. For any $x \in K$, we want to show that $|x|_2 = |x|_1^r$. Let s be the real number for which $|x|_1 = |y|_1^s$. We claim that $|x|_2 = |y|_2^s$. Granted the claim, we have $|x|_2 = |y|_2^s = |y|_1^{rs} = |x|_1^r$. Now we prove the claim. Take any rational number m/n, $n > 0$ greater than s. Then $|x|_1 = |y|_1^s < |y|_1^{m/n}$, and so $|x^n|_1 < |y^m|_1$, $|x^n/y^m|_1 < 1$. By assumption, $|x^n/y^m|_2 < 1$, $|x^n|_2 < |y^m|_2$ and so $|x|_2 < |y|_2^{m/n}$. It follows that $|x|_2 \leq |y|_2^s$. A similar argument with rationals m/n less than s shows that $|x|_2 \geq |y|_2^s$. Thus, $|x|_2 = |y|_2^s$, which proves the claim.

3 $\implies$ 1: obvious. □

Remark 17.9. Let K be a number field with ring of integers A. Then there is a bijection between prime ideals of A and equivalent classes of discrete abs vals on K: For a prime P, define $|a|_P := r^{-v_P(a)}$ where $r > 1$; conversely, for a given discrete abs val $|.|$, define $P := \{a \in A : |a| < 1\}$, then the valuation ring is A_P.

18. Completions

Let K be a field with a nontrivial abs val. A sequence (a_n) in K is called a Cauchy sequence if for every $\varepsilon > 0$ there is N such that $|a_m - a_n| < \varepsilon$ for all $m, n > N$. K is said to be complete w.r.t $||$ if every Cauchy sequence in K has a limit.

Exercise 18.1. (easy but important) If $|.|$ is nonarchimedean and $a_n \in K$ is Cauchy, then either $a_n \to 0$ or $|a_n|$ is constant for $n >> 0$.

We know from calculus that $\mathbb{Q}$ is not complete w.r.t the archimedean abs val $||_\infty$. Similarly, $\mathbb{Q}$ is not complete w.r.t. the standard p-adic absolute value $||_p$: one can see this by a cardinality argument as follows. Let a_n be an element of $\{0, 1, \cdots, p-1\}$, one for each $n \geq 0$. Consider the sum $\sum_{n\geq 0} a_n p^n$. As $|a_n|_p \leq 1$ and $|p^n|_p = \frac{1}{p^n}$, $|a_n p^n| \to 0$ as n goes to infinity, so the sequence of partial sums is Cauchy in $\mathbb{Q}$. By the argument in 18.4, no two different series can converge to the same limit (whenever they exist in $\mathbb{Q}$). Thus $\mathbb{Q}$ (being a countable set) cannot be complete w.r.t. $|.|_p$ since the set of all sums $\sum_{n\geq 0} a_n p^n$ is uncountable. One can also construct explicit Cauchy sequences in $\mathbb{Q}$ w.r.t. $||_p$ that do not have limits in $\mathbb{Q}$:

Example 18.2. Consider $\mathbb{Q}$ with the standard p-adic abs val $||_p$ ($p > 3$), i.e. $|x|_p = p^{-n}$ if $x = p^n \frac{u}{v}$ with u, v prime to p. Let a be an integer prime to p and is not congruent to ± 1 modulo p. Consider $(x_n := a^{p^n})$. By Fermat's Little Thm, $a^p \equiv a (p)$, so $a^{p^2} \equiv a^p (p^2)$, $a^{p^3} \equiv a^{p^2} (p^3)$, etc. It follows that $|x_{n+1} - x_n| \leq \frac{1}{p^{n+1}}$, and hence $|x_m - x_n| \leq \frac{1}{p^{n+1}}$ for $m > n$. Cauchy. If $\lim x_n = x$ for some $x \in \mathbb{Q}$, then $|x_n - x| \leq \frac{1}{p^{n+1}}$ (letting $m \to \infty$). In particular, letting $n = 0$, we get $|a - x| \leq 1/p$, i.e. $a \equiv x \mod p$. On the other hand, since $x_{n+1}^p = x_n$ for all n, $x^p = x$, which implies that $x = 0, \pm 1$ (there is no root of unity in $\mathbb{Q}$ other than ± 1). Thus $a \equiv 0, \pm 1 \mod p$, contradicting to our assumption on a.

Theorem 18.3. *Let K be a field with an abs val $||$. Then there exists a field $\hat{K}$ equipped with an abs val, also denoted $||$, and a map $i : K \to \hat{K}$ such that*

- *$\hat{K}$ is complete.*
- *i is an isometry with dense image.*
- *Any isometry $\phi : K \to E$ to a complete field factors uniquely through $\hat{K}$.*

Proof. Let $\mathcal{C}$ be the set of all Cauchy sequences in K. This is naturally a ring (not a field since there are Cauchy sequences converging to 0). Let $\mathcal{I} \subset \mathcal{C}$ be the set of sequences which converges to 0. Then $\mathcal{I}$ is an ideal. Moreover, the quotient ring $\mathcal{C}/\mathcal{I}$ is a field (as sequences not converging to 0 are eventually bounded away from 0, and hence invertible in $\mathcal{C}/\mathcal{I}$). We define an abs val on $\mathcal{C}$ by $|(x_n)| = \lim |x_n|$. This descends to $\mathcal{C}/\mathcal{I}$ and the natural map $K \to \mathcal{C}/\mathcal{I}$, $x \to (x, x, ...)$ is an isometry with dense image. We take $\hat{K} = \mathcal{C}/\mathcal{I}$. Then $\hat{K}$ is complete (WHY?). For any isometry $\phi : K \to E$ to a complete field, we can extend ϕ from K to $\hat{K}$ by mapping an element in $\hat{K}$, viewed as a Cauchy sequence in K, to the limit of its image in E (which exists since ϕ is an isometry and E is complete). □

For a number field K and a prime ideal P, we have the P-adic abs val $|a|_P = N(P)^{-v_P(a)}$ where $v_P(a) \in \mathbb{Z}$ is the exponent of P in the prime decomp of (a). We write K_P for the completion, and $\hat{O}_P := \{a \in K : v_P(a) \geq 0\}$ for the ring of integers in K_P. For example, $\mathbb{Q}_p$ is the completion of $\mathbb{Q}$ w.r.t. the p-adic abs val $||_p$ with ring of integers $\mathbb{Z}_p$.

Let $||$ be a discrete nonarchimedean abs val on K with corresponding valuation v, normalized so that $v(K^\times) = \mathbb{Z}$. Let π be an element of K such that $v(\pi) = 1$ (i.e. it is the smallest positive integer in $v(K^\times)$, or equivalently, it is the largest number in $|K^\times|$ that is < 1). Such a π is called a *uniformizer*. It generates the maximal ideal m of the valuation ring A (see the proof of 17.4).

Exercise 18.4. Show that for every element $x \in K^\times$, there exists an integer n, a unit $u \in A^\times$, such that $x = \pi^n u$.

Consider the completion $\hat{K}$ of K w.r.t. $||$.

Exercise 18.5. (A surprising fact) We have $|\hat{K}^\times| = |K^\times|$. Hint: go through the proof of 18.3 and use 18.1.

In particular, $||$ is a discrete abs val on $\hat{K}$. Let $\hat{A}$ be the d.v.r. associated with $||$ in $\hat{K}$ with maximal ideal $\hat{m}$, which is generated by the same element $\pi \in m$ by the above exercise.

Exercise 18.6. (see HW 7) Show that the residue field of $\hat{A}$ is the same as that of A.

We may think of elements in $\hat{K}$ as infinite series in π:

Proposition 18.7. *Choose a set $S \subset A$ of representatives for $k = A/m = \hat{A}/\hat{m}$.* [1] *Then every nonzero element in $x \in \hat{K}$ is of the form*

$$x = \sum_{i \geq n} a_i \pi^i$$

for some $n \in \mathbb{Z}$ and $a_i \in S$. Moreover, the coefficients are uniquely determined by x.

Proof. For any $x \in \hat{K}$, we can write $x = \pi^n u$ for $n \in \mathbb{Z}$ and $u \in \hat{A}^\times$. So wma $x \in A$. We construct recursively $(a_n) \in S$ such that $x \in a_0 + a_1\pi + ... + a_n\pi^n + (\pi)^{n+1}$ as follows: let $a_0 \in S$ be such that $x = a_0 + (\pi)$; suppose we have constructed $a_0, ..., a_n$, write $x = a_0 + a_1\pi + ... + a_n\pi^n + x_{n+1}\pi^{n+1}$ for $x_{n+1} \in \hat{A}$, and let a_{n+1} be an element in S such that $x_{n+1} \in a_{n+1} + (\pi)$; it follows that $x = a_0 + a_1\pi + ... + a_{n+1}\pi^{n+1} + (\pi^{n+2})$. It follows that $x = \sum_{i \geq 0} a_i \pi^i$. This proves the existence.

Uniqueness: for $k \in \mathbb{Z}$, if $\sum_{i \geq k} a_i \pi^i = \sum_{i \geq k} b_i \pi^i$, then division by π^k yields

$$(a_k - b_k) + (a_{k+1} - b_{k+1})\pi + \cdots = 0$$

In particular, $a_k - b_k \in m$. Since $a_k, b_k \in S$, this implies that $a_k = b_k$ and hence we can use induction to prove that $a_i = b_i$ for all $i \geq k$. □

A side note: observe that in contrast, the base 10 expansion of a real number is not unique. For instance, $1 = 0.99999\cdots$, i.e.

$$1 + 0\frac{1}{10} + 0\frac{1}{10^2} + \cdots = 0 + 9\frac{1}{10} + 9\frac{1}{10^2} + \cdots$$

19. Hensel's Lemon

20. Extensions of discrete abs vals

Theorem 20.1. *Let K be a* complete *field w.r.t. a discrete abs val $||_K$, and let L be a finite separable extension of K of degree n. Then $||_K$ extends uniquely to a discrete abs val $||_L$ on L, and L is complete w.r.t. $||_L$. In fact, we have*

$$|b|_L = |N_{L/K}(b)|_K^{1/n}.$$

Proof. Assuming the existence and uniqueness of the extension $||_L$, it is not hard to prove the above formula: $||_K$ extends uniquely to an abs val $||_L$ on L, and $||_L$ extends uniquely to an abs val $||_M$ of $M := L^{gal}$, the Galois closure of L in $\overline{K}$. For each K-embedding $\sigma : L \to M$, the map $b \to |\sigma b|_M$ is an abs val on $b \in L$, so $|\sigma b|_M = |b|_L$ by uniqueness. Thus,

$$|N_{L/K}(b)|_K = \prod |\sigma b|_M = |b|_L^n$$

where the product is taken over all the K-embeddings of L into M.

Existence and uniqueness: Let A be the d.v.r. in K and let B be the integral closure of A in L. Since A is a d.d, so is B (Milne, Theorem 3.29). Let P be the unique prime of A, then there exists a prime Q of B lying over P (by the going-up theorem in commutative

[1] More precisely, S is characterized by the following: for any $a \in A$, there is a unique $s \in S$ such that $a - s \in m$. In particular, if $s \neq s' \in S$, then $s - s' \notin m$.

algebra; alternatively, use Marcus p.40, Lemma 2 and the proof of Lemma 12.1 to show that $PB \neq B$, and hence is contained in a prime Q). Then the equivalent class of $||_K$ corresponds to P and the equivalent classes of discrete abs vals of L extending $||_K$ corresponds to primes Q lying over P (we need the unique factorization property of d.d. when going from primes to abs vals). So the existence of $||_L$ is proven. It remains to prove uniqueness.

Suppose there are distinct primes Q_1, Q_2 lying over P. Choose $b \in Q_1 - Q_2$, then $Q_1 \cap A[b] \neq Q_2 \cap A[b]$. So $A[b]$ has two primes lying over P. On the other hand, $A[b] = A[x]/(f(x))$ where $f(x) \in A[x]$ is the minimal polynomial of b over A. $\bar{f} \in k[x]$ ($k = A/P$) must be a power of an irrd: suppose $\bar{f} = \bar{g}\bar{h}$ with monic polynomials $(\bar{g}, \bar{h}) = 1$; since A is complete, Hensel's lemma implies that there exists $g, h \in A[x]$ such that $f = gh$, contradicting to the irrd of f. It follows that $A[b]/P \cong k[x]/(\bar{f}(x))$ is either a field or a d.v.r. In particular, $A[b]$ has only one prime ideal lying over P, a contradiction. It is not hard to see that L is complete w.r.t. $||_L$. □

Corollary 20.2. *Let K be as in the theorem, and let Ω be a possible infinite separable extension of K. Then $||_K$ extends in a unique way to an absolute value $||_\Omega$ on Ω.*

However,$||_\Omega$ may not be discrete and Ω is not necessarily complete w.r.t. $||_\Omega$.

Let K and L be as in the theorem with valuation rings A and B, and maximal ideals m_A and m_B. Let e be the integer for which $m_A B = m_B^e$, called the ramification index of L/K, and let f be $[B/m_B : A/m_A]$, called the residue class degree of L/K. Note that e equals the index of $|K^\times|_K$ in $|L^\times|_L$.

Definition 20.3. Say L/K is unramified if $e = 1$, and totally ramified if $f = 1$.

The following theorem is the local analog of a result we proved for Dedekind domains:

Theorem 20.4. *Let L/K and e, f be as above. Then $ef = n$.*

Exercise 20.5. Show that x^2+1 is irred over $\mathbb{Q}_3$. It follows that $L = \mathbb{Q}_3(\sqrt{-1})$ is a quadratic extension of $\mathbb{Q}_3$. Let $||$ be the valuation on L extending the 3-adic valuation.

(1) Show that for $a, b \in \mathbb{Q}_3$, $|a + b\sqrt{-1}| = \max(|a|, |b|)$.

(2) Determine $|K^\times|$, the valuation ring of K, and the residue field of K.

Exercise 20.6. Let p be a prime number. Show that $x^2 - p$ is irred over $\mathbb{Q}_p$. It follows that $L = \mathbb{Q}_p(\sqrt{p})$ is a quadratic extension of $\mathbb{Q}_p$. Let $||$ be the valuation on L extending the p-adic valuation.

(1) Show that for $a, b \in \mathbb{Q}_p$, $|a + b\sqrt{p}| = \max(|a|, \frac{1}{\sqrt{p}}|b|)$.

(2) Determine $|K^\times|$, the valuation ring of K, and the residue field of K.

21. Unramified extensions

Number theorists care about two kind of fields: global fields and local fields. A global field is by defn either a number field (i.e. a finite extension of Q) or a function field (i.e. a finite extension of $\mathbb{F}_p(t)$); a local field is by defn either one of $\mathbb{R}$, $\mathbb{C}$ (called archimedean local fields) or a field that is complete w.r.t. a discrete abs val whose residue field is finite

(called a nonarchimedean local field). For example, finite extensions of $\mathbb{Q}_p$, finite extensions of $\mathbb{F}_p((t))$. They arise as completions of number fields or function fields w.r.t. the absolute vals induced by their prime ideals.

Definition 21.1. A *nonarchimedean local fields* is a field K equipped with a nonarchimedean abs val |.| such that K is complete w.r.t |.| and the residue field of K is finite.

Given a nonarchimedean local field K with valuation ring A (**notational clarification: sometimes we write O_K for the valuation ring of K and call it the ring of integers of K. This is a justified use of language by the last exercise in HW 8**) and maximal ideal m and residue field $k = A/m = \mathbb{F}_q$ where q is a power of a prime number p (called the *residual characteristic of* K). Recall the Teichmuller isomorphism $[.] : k^\times \to \mu_{q-1}(K)$, where for any integer n we denote by $\mu_n(K)$ the group of n-th roots of unity in K. (Recall that [.] is obtained by applying Hensel's lemma to the polynomial $x^{q-1} - 1$, which relies on the completeness of K.)

Lemma 21.2. *Let α be a root of unity in K whose order is prime to $p := chark$, then $\alpha \in \mu_{q-1}(K)$.*

Proof. Suppose $\alpha^n = 1$ for n prime to p, then $\bar{\alpha}^n = \bar{1}$ in k, and hence $[\bar{\alpha}]^n = 1$ since [.] is a group homomorphism. As both α and $[\bar{\alpha}]$ reduces to $\bar{\alpha}$ mod m and $x^n - 1$ has no repeated roots in k (since n is prime to p!), we have $\alpha = [\bar{\alpha}] \in \mu_{q-1}(K)$. □

Recall that a finite extension L/K is unramified if its ramification index $e = 1$ (see 20.3). By 20.4, this is equivalent to $[L : K] = [k_L : k]$ with k_L the residue field of L.

Proposition 21.3. *Let K, A, k, p be as above. Let L/K be a finite extension generated by roots of unity of order prime to p. Then L/K is unramified.*

Proof. Let B be the valuation ring of L with residue field $k_L = B/m_B$. and $q_L := |k_L|$. By lemma, these roots of unity must be contained in $\mu_{q_L-1}(L) \cong k_L^\times$. So $L = K(\mu_{q_L-1}(L))$ (in particular L/K is Galois). Note that there is a natural group homom $\pi : \mathrm{Gal}(L/K) \to \mathrm{Gal}(k_L/k)$: for any $\sigma \in \mathrm{Gal}(L/K)$, σ induces an automorphism of B that fixes A, which (since $\sigma(m_B) \subset m_B$) descends to an autom $\bar{\sigma}$ of $B/m_B = k_L$ that fixes $k = A/m$. To show that L/K is unrd, STP π is injective (since $[k_L : k] | [L : K]$, injectivity will imply that $[k_L : k] = [L : K]$). Let σ be a nontrivial element in $\mathrm{Gal}(L/K)$, then (since $L = K(\mu_{q_L-1}(L))$) σ permutes the elements in $\mu_{q_L-1}(L)$ in a nontrivial way; since $\mu_{q_L-1}(L) \cong k_L^\times$ (Teichmuller isomorphism), it follows that $\bar{\sigma}$ permutes the elements in $k_L^\times$ in a nontrivial way.

Second proof: WMA $L = K(\zeta)$ for a root of unity ζ of order n not divisible by p. Let $f(x)$ be the (monic) minimal poly of ζ over K. Then $f(x) | x^n - 1$ and $f(x) \in A[x]$ (why?). Consider $\bar{f}(x) \in k[x]$. It divides $x^n - \bar{1}$, which is a separable poly in $k[x]$ as n is not divisible by p. It follows that $\bar{f}(x)$ is also separable and hence is irred over k by Hensel III. This implies that $\bar{f}(x)$ is the minimal poly of $\bar{\zeta} \in k_L$. We have $[k_L : k] \geq [k(\bar{\zeta}) : k] = \deg \bar{f} = \deg f = [L : K]$, and hence $[k_L : k] = [L : K]$. □

Proposition 21.4. *Let K, A, k, p be as above. Let L/K be an unrd finite extension. Let B be the valuation ring of L with residue field $k_L := B/m_B$ of cardinality q_L. Then $L = K(\mu_{q_L-1}(L))$.*

Proof. Let $L' := K(\mu_{q_L-1}(L)) \subset L$. Since p is prime to $q_L - 1$, the above prop implies that L'/K is unramified. Since the residue field of L' is visibly the same as that of L and L/K is unramified by assumption, it follows that $[L' : K] = [L : K]$ and hence $L' = L$. □

Corollary 21.5. *Given an integer f, K has a unique unrd extension of degree f. In fact, it is the cyclic extension obtained by adjoining to K the roots of $x^{q^f-1} - 1$ where $q = |k|$.*

Proof. Let L be the splitting field of $x^{q^f-1}-1$ over K. Then L/K is unrd (bc we are adjoining roots of unity of order prime to p), and if $\zeta \in L$ is a primitive $q^f - 1$ root of unity, then $\zeta \mapsto \zeta^q$ is a generator of $\mathrm{Gal}(L/K) \cong \mathrm{Gal}(k_L/k)$, whose order is f. This proves the existence. To prove uniqueness, suppose E is an unrd extension of K of degree f, then $[k_E : k] = f$ and hence $q_E = q^f$. The above prop then implies that $E = K(\mu_{q^f-1}(E))$, and hence E is the splitting field of $x^{q^f-1} - 1$ over K. □

Corollary 21.6. *The compositum of two unrd finite extensions of a local field K is again unrd.*

Proof. By the preceding two propositions, the compositum is generated by roots of unity of order prime to p, and hence is unramified. □

22. Totally ramified extensions

Let K be a nonarchimedean local field with O_K its ring of integers and m_K its maximal ideal. Let $k = O_K/m_K$ be the residue field of K. It is a finite field of order q, which is the power of some prime p. Denote by $v_K : K^\times \to \mathbb{Z}$ the *normalized* valuation of K (in the sense that v_K maps onto $\mathbb{Z}$). An absolute val on K is then of the form $|.|_K = r^{-v_K(.)}$ for some $r > 1$. A polynomial $f(x) = x^n + a_1x^{n-1} + ... + a_n \in O_K[x]$ is said to be *Eisenstein* if $v_K(a_i) > 0$ for all i and $v_K(a_n) = 1$. In other words, f is Eisenstein if $a_i \in m_K$ for all i and a_n is a uniformizer of K.

Exercise 22.1. Show that f is irred over O_K; then use Gauss lemma (see HW 1) to show that f is in fact irred over K. Hint: For the first part, consider the mod m reductions of its irred factors and argue by contradiction; for the second part, note that O_K is a d.v.r., in particular an UFD, to which Gauss's lemma applies.

Proposition 22.2. *Suppose L/K is a finite totally ramified extension of degree e with uniformizer ϖ_L, then the minimal polynomial of ϖ_L is Eisenstein of degree e and $L = K(\varpi_L)$;*

Conversely, if α is a root of an Eisenstein poly over O_K, then $L := K(\alpha)$ is a totally ramified extension with α an uniformizer of L.

Proof. Let us make a simple observation: if L/K is a finite extension with ramification index e and if $v_L : L^\times \twoheadrightarrow \mathbb{Z}$ is the normalized valuation on L, then $v_L = ev_K$ on K, and hence if $||_K = r^{-v_K(.)}$ for some $r > 1$ and $||_L$ extends $||_K$, then $||_L = r^{-\frac{v_L(.)}{e}}$.

For the first part, let $f(x) = x^n + a_1x^{n-1} + ... + a_n \in K[x]$ be the minimal poly of ϖ_L. Since $\varpi_L \in m_L$, we have $a_i \in m_K$ since a_i are symmetric polys of the conjugates of ϖ_L (check it). We need to show that $v_K(a_n) = 1$ and $n = e$. We have $|a_n|_K = |N_{K(\varpi_L)/K}(\varpi_L)|_K = |\varpi_L|_L^n$, so

the above formula gives $r^{-v_K(a_n)} = r^{-n\frac{v_L(\varpi_L)}{e}}$ and we get $ev_K(a_n) = n$. But $n \leq [L : K] = e$, this forces $e = n$ and $v_K(a_n) = 1$.

Conversely, if α is a root of $f(x) = x^n + a_1x^{n-1} + ... + a_n \in O_K[x]$ with $v(a_i) > 0$ and $v(a_n) = 1$ and $L = K(\alpha)$, then L/K is of degree n by irred of Eisenstein polys. Let e be the ramification index and f be the residue class degree, then $ef = n$. Just as above, we have $|a_n|_K = |\alpha|_L^n$, and so $r^{-v_K(a_n)} = r^{-n\frac{v_L(\alpha)}{e}}$, $nv_L(\alpha) = e$. But $e \leq ef = n$, this forces $n = e$ and $v_L(\alpha) = 1$, i.e. L/K is totally ramified and α is an uniformizer of L. □

23. Krasner's lemma and its applications

In this lecture, let K be a field that is complete w.r.t. a nonarchimedean abs val. We fix a separable algebraic closure $\bar{K}$ of K. Then $||$ extends uniquely to an abs val of $\bar{K}$, which we still denote by $||$ (recall the uniqueness relies on the completeness of K).

Lemma 23.1. *(Krasner's Lemma) Let $f \in K[x]$ be a monic polynomial with distinct roots $\alpha_i \in \bar{K}$. Suppose $\beta \in \bar{K}$ is an element such that $|\beta - \alpha_1| < \min_{i\neq 1}(|\alpha_i - \alpha_1|)$. Then $K(\alpha_1) \subset K(\beta)$.*

Proof. Let $L = K(\beta)$ and let M be $L(\alpha_1, ..., \alpha_n)$. STP for any $\sigma \in \mathrm{Gal}(M/L)$, $\sigma(\alpha_1) = \alpha_1$. We have $|\alpha_1 - \sigma(\alpha_1)| \leq \max(|\alpha_1 - \beta|, |\beta - \sigma(\alpha_1)|)$. Since $||$ is Galois invariant (which relies on the completeness of L) and $\beta \in L$, $|\beta - \sigma(\alpha_1)| = |\beta - \alpha_1| < \min_{i\neq 1}(|\alpha_i - \alpha_1|)$ (by assumption). It follows that $|\alpha_1 - \sigma(\alpha_1)| \leq \min_{i\neq 1}(|\alpha_i - \alpha_1|)$ which implies that $\sigma(\alpha_1) = \alpha_1$. □

For $f \in K[x]$, let $||f||$ be the maximum of the abs vals of its coefficients.

Lemma 23.2. *(Continuity of Roots) Let $\alpha \in \bar{K}$ be an element with minimal poly $f \in K[x]$ of degree n. Then for every $\epsilon > 0$ there is a $\delta > 0$ such that if $g \in K[x]$ is a monic poly of degree n such that $||g - f|| < \delta$, then g has a root β such that $|\beta - \alpha| < \epsilon$.*

Proof. Let $g \in K[x]$ be a monic poly of degree n with roots β_i. Then $|(f - g)(\alpha)| = |g(\alpha)| = \prod(\alpha - \beta_i)$. By choosing δ to be sufficiently small, we can guarantee that $|(f - g)(\alpha)| < \epsilon^n$, and hence for at least one i, $|\alpha - \beta_i| < \epsilon$. □

Corollary 23.3. *Let K be a field that is complete w.r.t. a nonarchimedean abs val. Let α and f be as in the lemma. Then for every $\epsilon > 0$ there is a $\delta > 0$ such that if $g \in K[x]$ is a monic poly of degree n such that $||g - f|| < \delta$, then g has a root β such that $K(\alpha) = K(\beta)$.*

Proof. This follows immediately from the above two lemmas. □

Corollary 23.4. *Let K be a nonarchimedean local field. Then, up to isomorphism, there are only finitely many extensions of K of a given degree contained in $\bar{K}$.*

Proof. Since every finite extension of K is an unramified extension followed by a totally ramified extension and K has a unique unramified extension of any given degree, STP the case when the extensions are totally ramified, i.e. those given by Eisenstein polys. Fix n and let $f(x) = x^n + a_1x^{n-1} + ... + a_n$ be an Eisenstein poly, which can be viewed as a point $(a_1, ..., a_n)$ in $m_K \times m_K \times ... \times m_K \times \mathcal{O}_K^\times \pi$. By the preceding corollary, each point has a neighbourhood such that the points in the neighbourhood all give the same extension of K.

As $m_K \times m_K \times ... \times m_K \times \mathcal{O}_K^\times \pi$ is compact (by HW 7, Exercise 2, since the residue field of K is assumed to be finite), it can be covered by finitely many such neighbourhoods. □

24. Absolute values of number fields

Theorem 24.1. *(Ostrowski) Let $||$ be a nontrivial abs val on $\mathbb{Q}$.*

(1) If $||$ is archimedean, then $||$ is equivalent to $||_\infty$.

(2) If $||$ is nonarchi, then $||$ is equivalent to $||_p$ for exactly one prime p.

Proof. We will not prove this in class. See Milne, Thm 7.12. □

Let K be a number field and let $||$ be a nontrivial abs val on K. If $||$ is archimedean, then its restriction to $\mathbb{Q}$ is equivalent to $||_\infty$ by Ostrowski, so $\hat{K}$, the completion of K w.r.t. $||$, is algebraic over $\mathbb{R}$ (the completion of $\mathbb{Q}$ w.r.t. $||_\infty$). It follows that $\hat{K}$ is isomorphic to one of $\mathbb{R}$ and $\mathbb{C}$. Moreover, $||$ is the restriction of $||_\infty$ (which denotes the standard abs val on $\mathbb{C}$ by abuse of notation) to K along some field embedding $\iota : K \to \mathbb{C}$. If $||$ is nonarchimedean, then its restriction to $\mathbb{Q}$ is equivalent to $||_p$ for some prime number p by Ostrowski, so $\hat{K}$, the completion of K w.r.t. $||$, is algebraic over $\mathbb{Q}_p$ (the completion of $\mathbb{Q}$ w.r.t. $||_p$). Moreover, $||$ is the restriction of $||_p$ (which denotes the unique extension of the standard p-adic abs val on $\mathbb{Q}_p$ to $\overline{\mathbb{Q}}_p$ by abuse of notation) to K along some field embedding $\iota : K \to \overline{\mathbb{Q}}_p$. This absolute value is associated to a prime ideal P of O_K above p in the sense that $|.| = r^{-v_P(.)}$ for some real number $r > 1$ (see 17.1 and 17.9).

Recall that two abs vals $||_1$ and $||_2$ on a field are equivalent if it satisfies one of the conditions in 17.8.

Definition 24.2. Let K be a field. A *place*, or a *prime* of K is defined to be an equivalent class of abs vals on K. A place is said to be archimedean, resp. nonarchimedean if the corresponding equivelant class of abs vals is archimedean, resp. nonarch.

Recall that a valuation on a field K is a map $v : K \to \mathbb{R} \cup \infty$ such that $v(0) = \infty$, $v(xy) = v(x) + v(y)$ for $x, y \in K^\times$ and $v(x + y) \geq \min(v(x), v(y))$ for $x, y \in K$. v is said to be discrete if $v(K^\times)$ is a lattice in $\mathbb{R}$. When K is a number field, for any prime ideal P of O_K, there is a natural discrete val v_P defined in 17.1. Recall that nonarch (resp. discrete nonarch) abs vals on a field K are in bijection with valuations (resp. discrete valuations) on K.

Important convention: We will typically use $v, w, ...$ to denote places of a field K, understood to be an equivalent class of abs vals on K. If v is nonarch, we may also think of it as a equivalent class of valuations on K. If K is a number field and v is a nonarch place of K (necessarily discrete), it is associated to a unique prime ideal of O_K. By abuse of notation, we sometimes use v to denote both the corresponding (equivalent class of) discrete valuation and the prime ideal, and use $||_v$ to denote the corresponding (equivalent class of) discrete abs val. We write K_v for the completion of K w.r.t. $||_v$ and call it *the completion of K at v.* Suppose L/K is a finite extension of number fields, let v, resp. w be a (possibly archimedean) place of K, resp. L. We say *w divides, or is above v*, denoted $w|v$, if $||_w$ extends $||_v$. When

the places are nonarch, this is equivalent to the prime ideal of O_L associated with w dividing the prime ideal of O_K associated with v.

Let K be a number field with a place v. Let L/K be a finite extension generated by $\alpha \in L$ whose minimal poly over K is denoted $f(x)$. Let w be place of L dividing v. Let K_v and L_w denote their completions. Then K_v is a subfield of L_w. Let $||_v$, resp. $||_w$ denote the abs vals on K_v, resp. L_w, extended from the corresponding abs vals on K, resp. L.

Lemma 24.3. $L_w = K_v(\alpha)$.

Proof. It is clear that $K_v(\alpha) \subset L_w$; on the other hand, since K_v is complete, $||_v$ extends to a *unique* abs val on $K_v(\alpha)$ and hence it equals the restriction of $||_w$ to $K_v(\alpha)$. Then $K_v(\alpha)$ is complete w.r.t. $||_w$. Since $L = K(\alpha) \subset K_v(\alpha)$, it follows that $L_w \subset K_v(\alpha)$. □

Proposition 24.4. *Let $L = K(\alpha)$ be a finite extension of a number field K with a place v and let $f(x)$ be the min poly of α over K. Then there is a bijection between the extensions of $||_v$ to L and the irrd factors of $f(x)$ in $K_v[x]$ (in other words, there is a bijection between the places of L dividing v and the irrd factors of $f(x)$ in $K_v[x]$).*

Proof. Let $g(x)$ be a monic irrd factor of $f(x)$ over K_v and let $\hat{L} := K_v[x]/g(x)$, then there is a natural injection $L = K[x]/f(x) \to \hat{L}$. Since K_v is complete, $||_v$ extends uniquely to an abs val $||$ on $\hat{L}$, which by restriction induces an abs val on L extending $||_v$.

Conversely, suppose $||$ is an extension of $||_v$ to L. Let $\hat{L}$ be the completion of L w.r.t. $||$. Then $\hat{L} = K_v(\alpha)$ by the lemma. Let $g(x)$ be the min poly of α (viewed as an element of $\hat{L}$ via the map $L \to \hat{L}$) over $\hat{K}$. Then $g(x)$ divides $f(x)$ and $\hat{L} = K_v(\alpha) = K_v[x]/g(x)$. □

Proposition 24.5. *Let K be a number field with a place v and let L/K be a finite extension. Then there are finitely many places w of L dividing v and we have*

$$L \otimes_K K_v \cong \prod_{w|v} L_w$$

Proof. Let $L = K(\alpha)$ for some $\alpha \in L$ with min poly $f(x) \in K[x]$. Then $f(x)$ factors in $K_v[x]$ as $f(x) = f_1(x)...f_g(x)$ for *distinct* irrd monic polynomials $f_i(x)$.

$$L \otimes_K K_v = K_v[x]/f(x) = \prod_i K_v[x]/f_i(x).$$

By the above prop, each $f_i(x)$ corresponds to a place $w_i|v$ for which $K_v[x]/f_i(x)$ is the completion of $L = K[x]/f(x)$ at w_i. □

Exercise 24.6. Let O_v be the valuation ring of K_v and let k_v be the residue field of K_v. Show that if $\alpha \in O_L$, then the monic polynomials $f_1, \cdots, f_g$ are actually in $O_v[x]$, and for each i, $\bar{f}_i$ is a power of an irred poly in $k_v[x]$. Hint: for the first part, use Gauss's lemma on polynomials; for the second part, use Hensel's lemma (which one?).

Corollary 24.7.

$$N_{L/K}(a) = \prod_{w|v} N_{L_w/K_v}(a)$$

$$\mathrm{tr}_{L/K}(a) = \sum_{w|v} \mathrm{tr}_{L_w/K_v}(a)$$

where $a \in L$ is regarded as an element of L_w via the embedding $L \to L_w$.

Proof. We only prove it for tr, the proof in the case of norm is similar. The multiplication by a map $m_a : L \to L$ is a K-linear map, which, tensored with $\hat{K}$, can be viewed as a $\hat{K}$-linear map

$$\tilde{m}_a : L \otimes_K \hat{K} \to L \otimes_K \hat{K}.$$

It is clear that $\mathrm{tr}\,\tilde{m}_a = \mathrm{tr}\,m_a$. On the other hand, since multiplication by a preserves each factor L_w of $L \otimes_K \hat{K} \cong \prod_{w|v} L_w$, $\mathrm{tr}\,\tilde{m}_a = \sum \mathrm{tr}\,\tilde{m}_a|_{L_w} = \sum \mathrm{tr}_{L_w/K_v}(a)$, and hence $\mathrm{tr}_{L/K}(a) = \mathrm{tr}\,m_a = \mathrm{tr}\,\tilde{m}_a = \sum \mathrm{tr}_{L_w/K_v}(a)$. □

25. Decomposition groups, inertia groups and the Frobenius element

L/K Galois. v a nonarch prime of K. $\mathrm{Gal}(L/K)$ acts transitively on $\{w|v\}$ by the proof of Corollary 12.5. The abs val $||_{\sigma w}$ is determined by $|\sigma(x)|_{\sigma w} = |x|_w$, i.e. $|x|_{\sigma w} = |\sigma^{-1}x|_w$. There is a natural K_v-isom induced by σ: $L_w \xrightarrow{\sim} L_{\sigma w}$: a Cauchy sequence $x_n \in L$ w.r.t. w maps to the Cauchy sequence $\sigma(x_n) \in L$ w.r.t. σw.

Lemma 25.1. *L_w/K_v is Galois.*

Proof. Let $L = K(\alpha)$, then $L_w = K_v(\alpha)$, where α is viewed as an element of L_w via the inclusion $L \to L_w$. Since L/K is Galois, the min poly of α over K splits in L. It follows that the min poly of α over K_v splits in L_w. □

Lemma 25.2. *Let $\sigma \in \mathrm{Gal}(L/K)$. Then σ extends to an element of $\mathrm{Gal}(L_w/K_v)$ iff $\sigma w = w$.*

Proof. $\Longrightarrow$: suppose σ extends to an element of $\mathrm{Gal}(L_w/K_v)$, then $||_{\sigma w} := |\sigma^{-1}()|_w$ is an abs val on L_w extending $||_v$; hence $||_{\sigma w} = ||_w$ by uniqueness.

$\Longleftarrow$: suppose $\sigma w = w$, then $L_w \xrightarrow{\sim} L_{\sigma w} = L_w$ defines an element of $\mathrm{Gal}(L_w/K_v)$. □

Definition 25.3. The decomposition group $D(w|v) := \{\sigma \in \mathrm{Gal}(L/K) : \sigma w = w\}$. The inertia group $I(w|v) := \{\sigma \in D(w|v) : \forall x \in O_L, \sigma(x) \equiv x \pmod{w}\}$.

Remark 25.4. There is a natural map $\pi : D(w|v) \to \mathrm{Gal}(k_w/k_v)$ with $k_v = O_K/v$ and $k_w = O_L/w$: for any $\sigma \in D(w|v)$, $\sigma(O_L) = O_L$ and $\sigma w = w$, so σ descends to a O_K/v-linear automorphism of O_L/w. We have $I(w|v) = \mathrm{Ker}\pi$.

We can interpret them in term of Galois groups of local fields.

Proposition 25.5. *There is a canonical injection $i_w : \mathrm{Gal}(L_w/K_v) \to \mathrm{Gal}(L/K)$ whose image is the decomposition group $D(w|v)$.*

Proof. For any $\sigma \in \mathrm{Gal}(L_w/K_v)$, since L/K is Galois, $\sigma(L) = L$, and we define $i_w(\sigma) = \sigma|_L$. If $i_w(\sigma)$ fixes L, then it fixes L_w since L is dense in L_w. So i_w is injective. That the image equals $D(w|v)$ follows immediately from the above lemma and the defn of $D(w|v)$. □

Proposition 25.6. $\sigma D(w|v)\sigma^{-1} = D(\sigma w|v)$, $\sigma I(w|v)\sigma^{-1} = I(\sigma w|v)$.

Proof. Exercise. □

Proposition 25.7. *There is a commutative diagram*

$$1 \to \mathrm{Gal}(L_w/L_w^{unr}) \to \mathrm{Gal}(L_w/K_v) \to \mathrm{Gal}(k(w)/k(v)) \to 1$$
$$1 \to I(w|v) \to D(w|v) \to \mathrm{Gal}(k(w)/k(v)) \to 1$$

where the horizontal sequences are exact, the vertical maps are isomorphisms, and L_w^{unr} is the maximal unramified subextension of L_w/K_v.

In particular, $I(w|v)$ is trivial iff L_w/K_v is an unramified extension of local fields, in which case $D(w|v) \cong \mathrm{Gal}(k(w)/k(v))$.

Proof. Observe that $k_w := O_L/w = O_{L_w}/m_{L_w}$ and $k_v := O_K/v = O_{K_v}/m_{K_v}$. The exactness of the top sequence then follows from HW 9, Problem 1. Since the middle vertical arrow is an isomorphism by Prop 25.5, it follows that the bottom sequence is exact and the left vertical arrow is an isomorphism. □

Proposition 25.8. *L/K not necessarily Galois. v a prime of K. Then*

(1) v is unramified in O_L iff for any $w|v$, L_w/K_v is an unramified extension of local fields.

(2) v splits completely in O_L iff for any $w|v$, $L_w = K_v$.

Proof. $e(L_w/K_v) = e(w|v)$, $f(L_w/K_v) = f(w|v)$ (HW 10, Problem 3) and $e(L_w/K_v)f(L_w/K_v) = [L_w : K_v]$ (Theorem 20.4). □

Theorem 25.9. *L/K, L'/K. v a place of K. Then v is unrd (resp. split) in LL' iff v is unrd (resp. split) in both L and L'.*

Proof. We only proof the unrd part and leave the split part as an exercise. $\Longrightarrow$ is obvious by definition. Conversely, if v is unrd in both L and L', need to show that for any place $\tilde{w}$ of LL' extending v, $(LL')_{\tilde{w}}/K_v$ is unrd. Let $w = \tilde{w}|_L$ and $w' = \tilde{w}|_{L'}$. Then $L_w L'_{w'} = (LL')_{\tilde{w}}$. In fact, it is clear that $L_w \subset (LL')_{\tilde{w}}$ and $L'_{w'} \subset (LL')_{\tilde{w}}$, and hence $L_w L'_{w'} \subset (LL')_{\tilde{w}}$; conversely, $L_w L'_{w'}$ (being a finite extension of the complete field K_v) is complete w.r.t. $||_{\tilde{w}}$ and contains LL', which imply that it contains the completion $(LL')_{\tilde{w}}$. By assumption, v is unrd in L and L', in particular, both L_w and $L'_{w'}$ are unramified over K_v. By local theory, the compositum $L_w L'_{w'} = (LL')_{\tilde{w}}$ is then unrd over K_v. □

26. The Frobenius elements and Chebotarev's density theorem

Definition 26.1. L/K Galois. $w|v$. Suppose that v is *unramified* in O_L. Define the *Frobenius element* $\mathrm{Fr}_{w|v} \in D(w|v)$ be the element corresponding to the Frobenius element in $\mathrm{Gal}(k_w/k_v)$ via the natural isomorphism $D(w|v) \cong \mathrm{Gal}(k_w/k_v)$. Equivalently, it is the *unique* element in $\mathrm{Gal}(L/K)$ such that

$$\mathrm{Fr}_{w|v}(x) \equiv x^{Nv} \pmod{w}$$

for all $x \in O_L$, where $Nv = |O_K/v| = |k_v|$.

Thus $\mathrm{Fr}_{w|v}$ generates $D(w|v) \cong \mathrm{Gal}(L_w/K_v)$.

Remark 26.2. For any $\sigma \in \mathrm{Gal}(L/K)$, $\sigma \mathrm{Fr}_{w|v} \sigma^{-1} = \mathrm{Fr}_{\sigma w|v}$. Denote by Fr_v this conjugacy class in the Galois group. When L/K is abelian, this conjugacy class becomes a single element in the Galois group.

Observation: v splits completely in L/K iff $\mathrm{Fr}_v = 1$. In fact, Prop 25.8, (2), v splits iff for any place w of L above v, $L_w = K_v$, which holds iff $\mathrm{Fr}_v = 1$.

Example 26.3. (1) Let $d \neq 1$ be a square-free integer. For $\mathrm{Gal}(\mathbb{Q}(\sqrt{d})/\mathbb{Q}) \cong \{\pm 1\}$ and $p \nmid 2d$, $\mathrm{Fr}_p = \left(\frac{d}{p}\right)$. Moreover, if 2 is unramified, then $\mathrm{Fr}_2 = 1$ iff $d \equiv 1 \mod 8$. See HW 5, Problem 5.

(2) For the cycl extension $\mathbb{Q}(\zeta_n)/\mathbb{Q}$, the Galois group $G \cong (\mathbb{Z}/n\mathbb{Z})^\times$ by Corollary 2.4. For $p \nmid n$, let P be a prime ideal of O dividing p, then $\mathrm{Fr}_{P|p}(\zeta) = \zeta^p$. In fact, let σ be the element in $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ for which $\sigma(\zeta) = \zeta^p$. By Theorem 6.4, $O = \mathbb{Z}[\zeta]$, it follows that $\sigma(x) \equiv x^p \mod P$ for all $x \in O$, and hence $\sigma = \mathrm{Fr}_{P|p}$.

Definition 26.4. Let K be a number field and let Σ_K be the set of nonarchimedean primes of K, and let S be a subset of Σ_K. The natural density of S is defined to be

$$\lim_{N\to\infty} \frac{|\{v \in S : Nv \leq N\}|}{|\{v \in \Sigma_K : Nv \leq N\}|},$$

whenever it exists.

Theorem 26.5. *(Chebotarev) Let L/K be a finite Galois extension of numebr fields. Let C be a conjugacy class in $G := \mathrm{Gal}(L/K)$. Then the set of primes v of K for which $\mathrm{Fr}_v = C$ has natural density $|C|/|G|$.*

In particular, every element in $\mathrm{Gal}(L/K)$ is of the form $\mathrm{Fr}_{w|v}$ for infinitely many primes v of K.

Corollary 26.6. *The set of primes v of K that splits completely in L has natural density $1/|G|$. In particular, there are infinitely many of them.*

27. Quadratic reciprocity

Theorem 27.1. *(Quadratic reciprocity) For odd primes p, q, $\left(\frac{q}{p}\right) = \left(\frac{p^*}{q}\right)$, where $p^* = (-1)^{\frac{p-1}{2}} p$. Moreover, $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.*

Proof. $G = \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^\times$. Let H be subgroup of G consisting of squares of the elements in G. Since G is cyclic and $2||G| = p - 1$, H is the unique index two subgroup of G. By an exercise in hwk 1, the fixed field of H is $\mathbb{Q}(\sqrt{p^*})$.

Let q be a prime different from p (q can be 2). Then q is unramified in $\mathbb{Q}(\zeta_p)$ (recall that its disc is a power of p). Consider Fr_q. It is an element in G (not just a conjugacy class since G is abelian). We have $\mathrm{Fr}_q(\zeta) = \zeta^q$ by Example 26.3, (2). Now $\left(\frac{q}{p}\right) = 1$ iff $q \in ((\mathbb{Z}/p\mathbb{Z})^\times)^2$ iff $\mathrm{Fr}_q \in H$ iff Fr_q fixes $\mathbb{Q}(\sqrt{p^*})$. Note that $\mathrm{Fr}_q|\mathbb{Q}(\sqrt{p^*})$ equals the Frobenius element of

$\mathrm{Gal}(\mathbb{Q}(\sqrt{p^*})/\mathbb{Q})$ at q, which equals (by Example 26.3, (1)) $\left(\frac{p^*}{q}\right)$ when $q \neq 2$. It follows that $\left(\frac{q}{p}\right) = 1$ iff $\left(\frac{p^*}{q}\right) = 1$ when $q \neq 2$. It remains to prove the case of $q = 2$. By Example, 26.3, (1), $\mathrm{Fr}_2|\mathbb{Q}(\sqrt{p^*}) = 1$ iff $p^* \equiv 1 \mod 8$, which holds iff $p \equiv 1, 7 \mod 8$. Thus the above equivalences imply that $\left(\frac{2}{p}\right) = 1$ iff $p \equiv 1, 7 \mod 8$. □

28. Kronecker-Weber

We will be following Sutherland's notes: `https://math.mit.edu/classes/18.785/2019fa/LectureNotes20.pdf`