

Math 225A Notes

Sarah Mantell

October 17, 2022

Algebraic Number Theory

1

1.1 General Definitions

Definition 1.1.1 (Number field): A number field is a finite field extension over \mathbb{Q} .

Definition 1.1.2 (Algebraic integer): Let K be a number field. An algebraic number $a \in K$ is called integral or an algebraic integer of K if $f(a) = 0$ for some monic polynomial f with coefficients in \mathbb{Z} . Denote the set of algebraic integers in K by \mathcal{O}_K .

Proposition 1.1.3: Let K be a number field. Then \mathcal{O}_K is a ring and $K = \text{Frac}(\mathcal{O}_K)$.

Proposition 1.1.4: The ring \mathcal{O}_K is Noetherian, integrally closed, and every nonzero prime ideal of \mathcal{O}_K is maximal.

Notice that the results presented in the proposition above imply that \mathcal{O}_K is a Dedekind domain, using one of the many equivalent definitions of a Dedekind domain.

Theorem 1.1.5 (Unique Factorization of Ideals): Every nonzero ideal $\mathfrak{a} \not\subseteq \mathcal{O}_K$ can be uniquely written as

$$\mathfrak{a} = \mathfrak{p}_1^{r_1} \cdots \mathfrak{p}_m^{r_m}$$

where $m \geq 1$, $\mathfrak{p}_1, \dots, \mathfrak{p}_m$ are distinct nonzero prime ideals of \mathcal{O}_K , and $r_1, \dots, r_m \in \mathbb{N}$.

Definition 1.1.6 (Trace, Norm): Suppose that $\mathbb{Q} \subseteq K \subseteq L$ is an extension of fields. Let $a \in L$ and view L as a K -vector space to consider the linear transformation

$$T_a : L \rightarrow L$$

1.1 General Definitions 1

1.2 Ramification 5

1.3 Valuations and Absolute Values 5
Completions 9

1.4 Absolute Values of Finite Extensions 10

1.5 Absolute Values of Number Fields 10

The notes here about algebraic number theory are very brief – the recommended texts for a more in depth reading are:

- Algebraic Number Theory Chapters I, II (Neukirch)
- Algebraic Number Theory Notes (Milne)

Theorem 1.1.5 is actually true for any Dedekind domain, but we just focus on this specific case here.

$$x \mapsto ax.$$

Define the trace and norm for a as

$$\mathrm{Tr}_{L/K}(a) = \mathrm{Tr}(T_a) \in K$$

and

$$\mathrm{Nm}_{L/K}(a) = \det(T_a) \in K.$$

With trace and norm defined as in Definition 1.1.6, we obtain a bi- K -linear pairing:

$$\langle \cdot, \cdot \rangle_{L/K} : L \times K \rightarrow K$$

given by

$$\langle a, b \rangle_{L/K} = \mathrm{Tr}_{L/K}(ab).$$

Definition 1.1.7: Let $\alpha_1, \dots, \alpha_n$ be a basis of L over K . The discriminant of $\alpha_1, \dots, \alpha_n$ is defined as

$$D(\alpha_1, \dots, \alpha_n) = \det \left((\langle \alpha_i, \alpha_j \rangle)_{1 \leq i, j \leq n} \right).$$

The discriminant of L/K is denoted by $D_{L/K}$ and is the ideal of \mathcal{O}_K generated by

$$\{D(\alpha_1, \dots, \alpha_n) : \alpha_1, \dots, \alpha_n \text{ is a basis of } L/K \text{ contained in } \mathcal{O}_L\}.$$

For K/\mathbb{Q} , $\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$ and therefore is a PID. So, \mathcal{O}_K is a free \mathbb{Z} -module of rank $n = [K : \mathbb{Q}]$. For any \mathbb{Z} -basis $\alpha_1, \dots, \alpha_n$ of \mathcal{O}_K ,

$$D_{K/\mathbb{Q}} = (D(\alpha_1, \dots, \alpha_n)).$$

The matrix

$$(\langle \alpha_i, \alpha_j \rangle)_{1 \leq i, j \leq n}$$

is an $n \times n$ matrix, with entries in K .

Definition 1.1.8 (Ramification index, Residue class degree/Intertia degree): Let L/K be an extension of number fields, $\wp \subseteq \mathcal{O}_L$ a nonzero prime ideal, and define $\mathfrak{p} = \wp \cap \mathcal{O}_K \subseteq \mathcal{O}_K$. Write the prime factorization of $\mathfrak{p}\mathcal{O}_L$ as

$$\mathfrak{p}\mathcal{O}_L = \wp_1^{e_1} \cdots \wp_m^{e_m}$$

where $\wp_1 = \wp$. The ramification index of \wp over \mathfrak{p} , denoted by $e(\wp/\mathfrak{p})$, is defined to be e_1 (as given in the prime factorization). The residue class degree, or the inertia degree, of \wp over \mathfrak{p} , denoted by $f(\wp/\mathfrak{p})$, is defined to be $[\mathcal{O}_L/\wp : \mathcal{O}_K/\mathfrak{p}]$.

Definition 1.1.9 (Ramified): Let L/K be an extension of number fields and $\mathfrak{p} \subseteq \mathcal{O}_K$ a nonzero prime ideal. We say \mathfrak{p} is ramified in L or L/K is ramified at \mathfrak{p} if $e(\mathfrak{p}/\mathfrak{p}) > 1$ for some $\mathfrak{p} \subseteq \mathcal{O}_L$ satisfying $\mathfrak{p} = \mathfrak{p} \cap \mathcal{O}_K$. We say \mathfrak{p} is unramified in L or L/K is unramified at \mathfrak{p} if $f(\mathfrak{p}/\mathfrak{p}) = 1$ for every $\mathfrak{p} \subseteq \mathcal{O}_L$ where $\mathfrak{p} = \mathfrak{p} \cap \mathcal{O}_K$.

Definition 1.1.10 (Splits, Splits completely): Let L/K be an extension of number fields and $\mathfrak{p} \subseteq \mathcal{O}_K$ a nonzero prime ideal. We say \mathfrak{p} splits or splits completely in L if $e(\mathfrak{p}/\mathfrak{p}) = f(\mathfrak{p}/\mathfrak{p}) = 1$ for every $\mathfrak{p} \subseteq \mathcal{O}_L$ with $\mathfrak{p} \cap \mathcal{O}_K = \mathfrak{p}$.

Definition 1.1.11 (Inert): Let L/K be an extension of number fields and $\mathfrak{p} \subseteq \mathcal{O}_K$ a nonzero prime ideal. We say that \mathfrak{p} is inert in L if $\mathfrak{p}\mathcal{O}_L$ is a prime ideal of \mathcal{O}_L .

From these definitions, one can derive the following identity: if $\mathfrak{p}\mathcal{O}_L = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_m^{e_m}$ then

$$[L : K] = \sum_{j=1}^m e(\mathfrak{p}_j/\mathfrak{p})f(\mathfrak{p}_j/\mathfrak{p}).$$

Theorem 1.1.12: The extension L/K is unramified at $\mathfrak{p} \subseteq \mathcal{O}_K$ if and only if \mathfrak{p} does not divide $D_{L/K}$. That is, $D_{L/K} \not\subseteq \mathfrak{p}$ if and only if \mathfrak{p} and $D_{L/K}$ are coprime ($\mathfrak{p} + D_{L/K} = \mathcal{O}_K$).

Theorem 1.1.13 (Minkowski): \mathbb{Q} has non nontrivial extension that is unramified at all primes. Equivalently, every $D_{K/\mathbb{Q}} \neq \pm 1$.

Note that Theorem 1.1.13 is not true for a general number field K :

Example 1: Let $K = \mathbb{Q}(\sqrt{-5})$ and $L = K(\sqrt{-1})$ so that L/K is an extension of number fields. Then, $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$ and $L = K(\sqrt{5})$. To see that L/K is unramified at all primes, we apply Theorem 1.1.12 and show that $D_{L/K} = \mathcal{O}_K$.

The remainder of this example is just some computations regarding the discriminant and two different K -bases of L .

Definition 1.1.14 (Fractional ideal): A fractional ideal of K is a nonzero finitely generated \mathcal{O}_K -submodule of K .

One can define a multiplication on the collection of fractional ideals of K : if $\mathfrak{a}_1, \dots, \mathfrak{a}_n$ are all fractional ideals of K , then the product is the \mathcal{O}_K -submodule of K generated by $\{a_1 \cdots a_n | a_j \in \mathfrak{a}_j\}$.

Proposition 1.1.15: The collection of fractional ideals of K forms an abelian group under the multiplication of fractional ideals. With this structure, the identity is \mathcal{O}_K and the inverse of \mathfrak{a} is $\mathfrak{a}^{-1} = \{x \in K | x\mathfrak{a} \subseteq \mathcal{O}_K\}$.

Proposition 1.1.16: Let K be a number field. Every fractional ideal \mathfrak{a} of K can be written uniquely in the form

$$\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{r_{\mathfrak{p}}}$$

where the product is taken over all the nonzero prime ideals of \mathcal{O}_K , each $r_{\mathfrak{p}} \in \mathbb{Z}$, and almost every $r_{\mathfrak{p}}$ is zero.

Remark 1 With these definitions, I_K is the free abelian group on the set of nonzero prime ideals of \mathcal{O}_K .

Define a subgroup of I_K by

$$P_K = \{(a) = a\mathcal{O}_K : a \in K^\times\}.$$

Definition 1.1.17 (Ideal class group, Class group): The ideal class group or class group of K is defined as

$$\text{Cl}(K) = I_K / P_K.$$

Theorem 1.1.18: For any number field K , the class group $\text{Cl}(K)$ is finite.

Definition 1.1.19 (Class number): The class number of a number field K is the order of the class group $\text{Cl}(K)$.

The proof that the class number of a given number field is indeed finite uses Minkowski Theory.

For a number field K , let r_k denote the number of real embeddings of K into \mathbb{R} and s_k denote the number of pairs of complex embeddings of K into \mathbb{C} . Here we are assuming that s_k is counting the pairs of embeddings that are not strictly contained in \mathbb{R} . Note that the complex embeddings occur in pairs through complex conjugation.

Theorem 1.1.20 (Dirichlet's Unit Theorem): Suppose that K is a number field and $\mu(K)$ is the finite group of roots of unity that are contained in K . Then,

$$\mathcal{O}_K^\times \cong \mathbb{Z}^{r_k+s_k-1} \times \mu(K).$$

Definition 1.1.21 (Decomposition group): Suppose that L/K is a Galois extension of number fields, $\wp \subseteq L$ is a prime ideal, and $\mathfrak{p} = \wp \cap \mathcal{O}_K$. The decomposition group of \wp is the set

$$G_\wp = \{\sigma \in \text{Gal}(L/K) : \sigma(\wp) = \wp\}.$$

Definition 1.1.22 (Inertia group): Let $\kappa = \mathcal{O}_K/\mathfrak{p}$ and $\lambda = \mathcal{O}_L/\wp$. The kernel of the map

$$G_\wp \rightarrow \text{Aut}(\lambda/\kappa)$$

is the inertia group of \wp and is denoted by I_\wp .

Need to check the assumptions here – where is \wp living? Nonzero?

1.2 Ramification

Theorem 1.2.1: Let L/K and K'/K be two extensions lying within an algebraic closure \bar{K}/K . Define $L' = LK'$. If L/K is unramified, then L'/K' is unramified. That is, every subextension of an unramified extensions is unramified.

1.3 Valuations and Absolute Values

In general, assume hereafter that p denotes some prime number.

Definition 1.3.1 (p -adic absolute value, p -adic norm): The p -adic absolute value or norm of \mathbb{Q}

$$|\cdot|_p : \mathbb{Q} \rightarrow \mathbb{R}$$

is defined by

$$\left| p^m \frac{a}{b} \right|_p = p^{-m}$$

where both a and b are coprime to p . Set $|0|_p = 0$.

Proposition 1.3.2: The p -adic norm is indeed a norm. That is:

1. $|a|_p > 0$ for all $a \in \mathbb{Q}^\times$
2. $|ab|_p = |a|_p |b|_p$
3. $|a + b|_p \leq |a|_p + |b|_p$

The p -adic norm actually satisfies a stronger version of the triangle inequality: $|a + b|_p \leq \max\{|a|_p, |b|_p\}$. Since we have now equipped \mathbb{Q} with a norm, it can be viewed as a topological space and thus there is a notion of convergence and Cauchy sequences. In particular, we are interested in studying the completion of \mathbb{Q} with respect to a given p -adic norm.

Definition 1.3.3 (p -adic numbers): Let \mathbb{Q}_p be the completion of \mathbb{Q} with respect to the p -adic norm. The elements of \mathbb{Q}_p are called the p -adic numbers.

Using properties of limits and the fact that every element of \mathbb{Q}_p can be represented as the limit of a sequence of points in \mathbb{Q} , the addition and multiplication of \mathbb{Q} can be naturally extended to \mathbb{Q}_p . Likewise, the norm $|\cdot|_p$ can be extended to a norm on \mathbb{Q}_p . With these operations, \mathbb{Q}_p is a field that contains \mathbb{Q} as a subfield.

Definition 1.3.4 (p -adic integers): Define the ring of p -adic integers to be the subset of \mathbb{Q}_p given by

$$\mathbb{Z}_p = \{a \in \mathbb{Q}_p : |a|_p \leq 1\}.$$

One can easily see that the set of units is $\mathbb{Z}_p^\times = \{a \in \mathbb{Q}_p : |a|_p = 1\}$.

Example 2: The polynomial $x^{p-1} - 1$ is solvable of \mathbb{Q}_p .

Definition 1.3.5 (p -adic valuation): The p -adic valuation of \mathbb{Q} is given by

$$v_p : \mathbb{Q} \rightarrow \mathbb{R} \cup \{\infty\}$$

where $v_p(p^m \frac{a}{b}) = m$ and both a and b are coprime to p . The p -adic valuation can be extended to \mathbb{Q}_p by letting $v_p(p^m a) = m$ where $a \in \mathbb{Z}_p^\times$.

Proposition 1.3.6: The p -adic valuation satisfies the following:

1. $v_p(a) = \infty$ if and only if $a = 0$
2. $v_p(ab) = v_p(a) + v_p(b)$
3. $v_p(a + b) = \min\{v_p(a), v_p(b)\}$

Furthermore, the p -adic valuation and p -adic absolute value have the following relation:

$$|a|_p = p^{-v_p(a)} \quad v_p(a) = -\log_p |a|_p.$$

Definition 1.3.7 (Absolute value, Nonarchimedean): An absolute value, or multiplicative valuation, of a field K is a function $|\cdot| : K \rightarrow \mathbb{R}_{\geq 0}$ such that

- (1) $|x| = 0$ if and only if $x = 0$
- (2) $|xy| = |x| \cdot |y|$
- (3) $|x + y| \leq |x| + |y|$

If instead of (3), the stronger condition

$$|x + y| \leq \max\{|x|, |y|\}$$

holds, then $|\cdot|$ is a nonarchimedean absolute value.

Definition 1.3.8 (Equivalent): Two absolute values are equivalent if they induce the same topology.

Using topological properties, one can show that two absolute values $|\cdot|_1, |\cdot|_2$ on K are equivalent if and only if there exists $s \in \mathbb{R}_{>0}$ such that $|x|_1 = |x|_2^s$ for all $x \in K$. In particular, if there exists $x \in K$ where $|x|_1 \geq 1$

and $|x|_2 < 1$ the two absolute values are *not* equivalent.

Definition 1.3.9 (Additive valuation, Valuation): An additive valuation on a field K is a function $v : K \rightarrow \mathbb{R} \cup \{\infty\}$ such that

- (1) $v(x) = \infty$ if and only if $x = 0$
- (2) $v(xy) = v(x) + v(y)$
- (3) $v(x + y) \geq \min\{v(x), v(y)\}$.

With these definitions, the collection of valuations and collection of nonarchimedean absolute values are related by the exponential and logarithmic functions. With this relationships, we can define the following:

Definition 1.3.10 (Equivalent valuations): Two valuations are equivalent if their corresponding absolute values are equivalent (see Definition 1.3.8).

Theorem 1.3.11: Every absolute value of \mathbb{Q} is either the usual Euclidean absolute value or is equivalent to $|\cdot|_p$ for some prime p .

From hereafter, $|\cdot|_\infty$ is used to denote the Euclidean absolute value.

Definition 1.3.12 (Residue class field, Valuation ring): Let K be a field with valuation v . The local ring¹

$$\mathcal{O} = \{x \in K : v(x) \geq 0\}$$

is the valuation ring for K . The unique maximal ideal of \mathcal{O} is

$$\mathfrak{p} = \{x \in K : v(x) > 0\}$$

the units are

$$\mathcal{O}^\times = \{x \in K : v(x) = 0\}$$

The field \mathcal{O}/\mathfrak{p} is the residue class field of \mathcal{O} .

1: A **local ring** is a ring with a unique maximal ideal.

Definition 1.3.13 (Discrete valuation): A valuation v on K is called discrete if $v(K^\times) = s\mathbb{Z}$ for some $s \in \mathbb{R}_{>0}$.

Definition 1.3.14 (Uniformizer): Assume that v is a discrete valuation with $v(K^\times) = s\mathbb{Z}$. An element $\varpi \in K$ is a uniformizer if $v(\varpi) = s$.

Alternatively, we can think of the uniformizer as follows: ϖ is a uniformizer if and only if ϖ generates the unique maximal ideal of the valuation ring.

If v is a discrete valuation, then it can be normalized to a valuation $v'(x) = s^{-1}v(x)$. From this definition, v and v' are equivalent and $v'(K^\times) = \mathbb{Z}$. Once normalized, an element ϖ is a uniformizer if and only if $v'(\varpi) = 1$.

Proposition 1.3.15: Let K be a field with a discrete valuation. Then, the corresponding valuation ring is a discrete valuation ring ².

2: A discrete valuation ring is a local PID that is not a field.

Completions

Now that a field K can be equipped with a norm, we can construct a completion of K with respect to any p -adic norm. The definition of completeness is the usual:

Definition 1.3.16 (Complete): The pair $(K, |\cdot|)$ is complete if every Cauchy sequence converges in K (with respect to the $|\cdot|$ norm.)

Given any $(K, |\cdot|)$, we can always find a completion \hat{K} and naturally extend $|\cdot|$ to \hat{K} . This new pair, $(\hat{K}, |\cdot|)$ is a complete valued field. When the absolute value $|\cdot|$ is nonarchimedean, the natural embedding

$$\mathcal{O}_K/\mathfrak{p} \hookrightarrow \mathcal{O}_{\hat{K}}/\mathfrak{p}_{\hat{K}}$$

of residue classes is an isomorphism.

Example 3: The completion of \mathbb{Q} with respect to $|\cdot|_\infty$ is \mathbb{R} . The completion of \mathbb{Q} with respect to $|\cdot|_p$ is \mathbb{Q}_p .

Theorem 1.3.17 (Hensel's Lemma): Let K be a complete discrete valued field with valuation ring \mathcal{O} and maximal ideal \mathfrak{p} . Suppose that a polynomial $f(x) \in \mathcal{O}[x] - \mathfrak{p}[x]$ can be factored as

$$\overline{f}(x) = \overline{g}(x)\overline{h}(x)$$

in $\mathbb{O}/\mathfrak{p}[x]$, with $\bar{g}(x)$ and $\bar{h}(x)$ coprime. Then, $f(x)$ has a factorization

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

in $\mathbb{O}[x]$ such that $g(x) \equiv \bar{g}(x) \pmod{\mathfrak{p}}$, $h(x) \equiv \bar{h}(x) \pmod{\mathfrak{p}}$, $\deg(g(x)) = \deg(\bar{g}(x))$, and $\deg(h(x)) = \deg(\bar{h}(x))$.

1.4 Absolute Values of Finite Extensions

Theorem 1.4.1: Let K be a field complete with respect to $|\cdot|$. Then $|\cdot|$ can be extended uniquely to an absolute value on any finite extension L of K by setting

$$|\alpha| = |\mathrm{Nm}_{L/K}(\alpha)|^{\frac{1}{[L:K]}}$$

for each $\alpha \in L$.

One can check that L is complete with respect to the defined norm. Also, if K is a field complete with respect to some $|\cdot|$, then every element of $\mathrm{Aut}(L/K)$ is a homeomorphism of L with respect to the extension of $|\cdot|$. Finally, $|\cdot|$ can be extended uniquely to an absolute value on \bar{K} . However, it's not necessarily the case that \bar{K} is complete with respect to the extension of the absolute value.

1.5 Absolute Values of Number Fields

Suppose that K is a number field and \mathfrak{p} is a nonzero prime ideal of \mathbb{O}_K . Then, the localization ³ of \mathbb{O}_K at \mathfrak{p} is a PID. This follows from the fact that \mathbb{O}_K is a Dedekind domain and any local Dedekind domain is a PID.

Since the localization, say $\mathbb{O}_{K,\mathfrak{p}}$, is a PID we may choose a generator ω of $\mathfrak{p}\mathbb{O}_{K,\mathfrak{p}}$. Then,

$$\mathbb{O}_{K,\mathfrak{p}} = \{0\} \cup \bigcup_{m \geq 0} \omega^m \mathbb{O}_{K,\mathfrak{p}}^\times$$

and

3: In general, if I is a prime ideal of a ring R , then one can define the localization of R at I by defining $S = R \setminus I$ and considering the ring of fractions $S^{-1}R$.

$$K = \{0\} \cup \bigcup_{m \in \mathbb{Z}} \varpi^m \mathcal{O}_{K, \mathfrak{p}}^\times.$$

Definition 1.5.1 (*p*-adic absolute value, *p*-adic norm): Define the *p*-adic absolute value or norm

$$|\cdot|_{\mathfrak{p}} : K \rightarrow \mathbb{R}_{\geq 0}$$

by

$$|\varpi^m a|_{\mathfrak{p}} = |\mathcal{O}_K / \mathfrak{p}|^{-m}$$

where $m \in \mathbb{Z}$ and $a \in \mathcal{O}_{K, \mathfrak{p}}^\times$. Set $|0|_{\mathfrak{p}} = 0$.

Theorem 1.5.2: Every nontrivial absolute value of a number field K is either equivalent to $|\cdot|_{\mathfrak{p}}$ for some nonzero prime ideal \mathfrak{p} of \mathcal{O}_K or some composition $|\cdot|_{\mathbb{C}} \circ \tau$ with $\tau : K \rightarrow \mathbb{C}$.

Theorem 1.5.2 can be thought of as a generalization of Theorem 1.3.11. The definitions for the *p*-adic norm replicate the construction of the *p*-adic norm and the *p*-adic integers. However, instead of restricting ourselves to prime numbers, we are now able to consider prime ideals.

Definition 2.0.1 (Local field): A local field is a field K with a nontrivial absolute value $|\cdot|$ such that K is locally compact with respect to $|\cdot|$.

Requiring that K is locally compact with respect to $|\cdot|$ implies that K is complete with respect to $|\cdot|$. If $K = \mathbb{R}$ or $K = \mathbb{C}$, then K is an archimedean local field. If the corresponding $|\cdot|$ has a discrete valuation with finite residue class field, then K is a nonarchimedean local field.

Definition 2.0.2 (Global field): A global field is either:

- (1) An algebraic number field.
- (2) A function field in one variable over a finite field.

A number field is always characteristic zero as it is defined as an extension over \mathbb{Q} . If the function field of an algebraic curve is taken over a finite field, it is the same as viewing it as a finite extension of some $\mathbb{F}_p(t)$ which is of nonzero (prime) characteristic.

Proposition 2.0.3: A local field is the completion of some global field with respect to an absolute value.

Class field theory describes relationships between the abelian extensions of a number field K and the structure of \mathcal{O}_K .

Definition 2.0.4 (Unramified abelian extension): A maximal unramified abelian extension of K is an extension L that is unramified at all primes and every real embedding $K \hookrightarrow \mathbb{R}$ extends to a real embedding $L \hookrightarrow \mathbb{R}$.

Theorem 2.0.5: Let L be a maximal unramified abelian extension of K . Then there exists a canonical isomorphism

$$\text{Cl}(K) \xrightarrow{\cong} \text{Gal}(L/K).$$

The canonical isomorphism in Theorem 2.0.5 can be described as follows:

Not sure exactly what was being defined here... Should revisit later.

Consider the diagram:

$$\begin{array}{ccccc} L & \xrightarrow{\cong} & \mathcal{O}_L & \xrightarrow{\cong} & \wp \\ | & & & & \\ K & \xrightarrow{\cong} & \mathcal{O}_K & \xrightarrow{\cong} & \mathfrak{p} \end{array}$$

where \wp is a nonzero prime ideal of \mathcal{O}_L and $\mathfrak{p} = \wp \cap \mathcal{O}_K$. Define $\lambda = \mathcal{O}_L/\wp$ and $\kappa = \mathcal{O}_K/\mathfrak{p}$. There exists a natural map

$$G_\wp \rightarrow \text{Aut}(\lambda/\kappa)$$

If $\sigma \in G_\wp \subseteq \text{Gal}(L/K)$ then $\sigma(\wp) = \wp$ (and in particular, $\sigma(\mathfrak{p}) = \mathfrak{p}$). Define an element φ_σ of $\text{Aut}(\lambda/\kappa)$ by

$$\varphi_\sigma : x + \wp \mapsto \sigma(x) + \wp$$

noting that this map is well-defined since \wp is fixed by σ . Furthermore, as σ fixes elements in K , φ_σ fixes elements of κ . Therefore, the map $G_\wp \rightarrow \text{Aut}(\lambda/\kappa)$ given by $\sigma \mapsto \varphi_\sigma$ is as desired.

If K_1/K and K_2/K are both unramified abelian extensions, then K_1K_2/K is an unramified abelian extension (see Theorem 1.2.1). This means that the maximal unramified abelian extension of K can be well defined as the composition of all unramified abelian extensions of K .

Definition 2.0.6 (Hilbert class field): Let K be a number field. The maximal unramified abelian extension of K is called the Hilbert class field.

Assuming the same notation and set up as 2, we have the following result:

Proposition 2.0.7: An extension L/K is unramified if and only if the natural map $G_\wp \rightarrow \text{Aut}(\lambda/\kappa)$ is an isomorphism.

Proof. Note that $\mathfrak{p}\mathcal{O}_L$ has a unique factorization of the form:

$$\mathfrak{p}\mathcal{O}_L = \wp_1^{e_1} \cdots \wp_r^{e_r}$$

with $\wp_1 = \wp$. Consider the following two facts:

Remark 2 Need to add more details for the proof here – a lot is missing.

- (1) $[L : K] = \sum_{j=1}^r e(\wp_j/\mathfrak{p})f(\wp_j/\mathfrak{p})$.
 (2) The Galois group $\text{Gal}(L/K)$ acts transitively on the collection $\{\wp_1, \dots, \wp_r\}$.

Fact (2) means that there is a bijection between $\{\wp_1, \dots, \wp_r\}$ and the G_\wp -cosets in $\text{Gal}(L/K)$. That is,

$$r = \frac{|\text{Gal}(L/K)|}{|G_\wp|} = \frac{[L : K]}{|G_\wp|}.$$

Combining this with fact (1) yields

$$[L : K] = r$$

and since $r = \frac{[L:K]}{|G_\wp|}$,

$$|G_\wp| = e(\wp/\mathfrak{p})f(\wp/\mathfrak{p}) = e(\wp/\mathfrak{p})[\lambda : \kappa].$$

□

Suppose that \mathfrak{p} is unramified in L/K . Proposition 2.0.7 implies that there is an isomorphism between G_\wp and $\text{Gal}(\lambda/\kappa)$. The Galois group is cyclic and thus has a generator $\text{Fr} : \lambda \rightarrow \lambda$ where $\text{Fr} : x \mapsto x^{|\kappa|}$. This generator is called the **Frobenius element** and is denoted by Frob_\wp .

As the Galois group $\text{Gal}(L/K)$ acts transitively on the collection of prime ideals lying above \mathfrak{p} , given any $\wp' \subseteq \mathcal{O}_L$ lying above \mathfrak{p} , there exists $\sigma \in \text{Gal}(L/K)$ with $\wp' = \sigma(\wp)$. It can be verified that

$$\text{Frob}_{\wp'} = \sigma \text{Frob}_\wp \sigma^{-1}$$

meaning that Frob_\wp and $\text{Frob}_{\wp'}$ are in the same conjugacy class in $\text{Gal}(L/K)$. This means that the following definition is well-defined:

Definition 2.0.8 (Frobenius of \mathfrak{p}): Let \mathfrak{p} and \wp be nonzero prime ideals such that $\mathfrak{p} = \wp \cap \mathcal{O}_K$. The Frobenius of \mathfrak{p} , denoted by $\text{Frob}_\mathfrak{p}$, is the conjugacy class of $\text{Gal}(L/K)$ that contains Frob_\wp .

When L/K is an abelian extension, the conjugacy class is a single element. Therefore, instead of referring to the conjugacy class as the Frobenius of \mathfrak{p} , we refer to the element in the conjugacy class as the Frobenius of \mathfrak{p} . We maintain the same notation.

I'm confused on the first couple lines of the proof here. Why do we know that the ramification indexes are all equal? How does transitivity give a relationship to the G_\wp cosets in $\text{Gal}(L/K)$?

When L/K is an unramified abelian extension, then the group homomorphism

$$I_K \rightarrow \text{Gal}(L/K)$$

with

$$\mathfrak{p} \mapsto \text{Frob}_{\mathfrak{p}}$$

is well-defined. This motivates the following theorem:

Theorem 2.0.9: Suppose that L is the maximal unramified abelian extension of K . Then the group homomorphism $I_K \rightarrow \text{Gal}(L/K)$ is surjective and has kernel P_K .

Corollary 2.0.10: Let \mathfrak{p} be a prime ideal of K and L the Hilbert class field of K . Then, \mathfrak{p} splits in L if and only if \mathfrak{p} is a principal ideal.