# MATH 223A: ALGEBRAIC NUMBER THEORY

WERN JUIN GABRIEL ONG

## Preliminaries

These notes roughly correspond to the course **MATH 223A: Algebraic Number Theory** taught by Prof. Melanie Wood at Harvard University in the Fall 2023 semester. These notes are LaTeX-ed after the fact with significant alteration and are subject to misinterpretation and mistranscription. Use with caution. Any errors are undoubtedly my own and any virtues that could be ascribed to these notes ought be attributed to the instructor and not the typist.

## Contents



## 1. Lecture 1 – 11th September 2023

This is a first graduate course in algebraic number theory. We will study local fields.

Let us understand the what and why of local fields. Local fields are interesting in the context of global fields. Let us consider some examples of global fields.

**Example 1.1** (Number Fields)**.** $K/\mathbb{Q}$ where $[K:\mathbb{Q}] < \infty$, finite extensions of $\mathbb{Q}$.

**Example 1.2** (Function Fields)**.** Function fields of curves over finite fields $\mathbb{F}_q$.

One's first study of number theory seeks to treat $\mathbb{Z} \subseteq \mathbb{Q}$, but there is a strong analogy between studying $\mathbb{Z} \subseteq \mathbb{Q}$ and $\mathbb{F}_q[t] \subseteq \mathbb{F}_q(t)$. In particular, one can show that there is a bijection betwween smooth geometrically irreducible curves over $\mathbb{F}_q$ up to isomorphism and finite extensions of $\mathbb{F}_q(t)$ up to isomorphism.

**Example 1.3.** The field $\mathbb{F}_q(t)$ is the field of rational functions of $\mathbb{P}^1_{\mathbb{F}_q}$.

This is an example of the function field analogy, drawing connections between geometry over finite fields $\mathbb{F}_q$ and $\mathbb{C}$. In fact, function fields and number fields are the only examples of global fields. This was first studied in the 20th century through the study of class field theory, field extensions with Abelian Galois group, that saw similar methods applied to number fields and function fields of $C_{/\mathbb{F}_q}$. Artin-Whaples axiomatized what was special about function fields and number fields by defining global fields and valuations. This led to a new approach to proving Dirichlet's unit theorem in the 1940s. Valuations will be our starting point for this class.

**Definition 1.4** (Valuation)**.** Let $K$ be a field. A valuation on $K$ is a function $|\cdot| : K \to \mathbb{R}$ such that:

(a) $|x| \geq 0$ for all $x \in K$ and $|x| = 0$ if and only if $x = 0$,
(b) $|xy| = |x| \cdot |y|$,

(c) and $|x+y| \leq |x| + |y|$.

Let us consider some valuations of fields.

**Example 1.5** (Trivial Valuation)**.** There is a trivial valuation

$$\begin{cases} |x| = 0 & x = 0 \\ |x| = 1 & x \neq 0 \end{cases}$$

on $K$.

We can see that both $\mathbb{R}$ and $\mathbb{C}$ are fields with the "standard" valuations. Let $K$ be a number field. $K$ admits homomorphisms to $\mathbb{R}$ and/or $\mathbb{C}$ and inherits the absolute value from $\mathbb{R}$ and/or $\mathbb{C}$. More precisely, if $[K : \mathbb{Q}] = n$, there are $n$ homomorphisms to $\mathbb{C}$ giving $n$ possibly distinct valuations on $K$.

**Example 1.6.** The field $\mathbb{Q}(i)$ is of degree $[\mathbb{Q}(i) : \mathbb{Q}] = 2$. $\mathbb{Q}(i)$ has two maps to $\mathbb{C}$, by $i \mapsto i$ and $i \mapsto -i$, each of which defines a norm on $\mathbb{Q}(i)$.

For any number field, each conjugate of a generator defines a homomorphism to $\mathbb{C}$.

**Example 1.7** ($\wp$-adic Valuation)**.** Let $K$ be a number field and $\mathcal{O}_K$ be its ring of algebraic integers. Let $\wp$ be a prime ideal of $\mathcal{O}_K$. For each $x \in K$, $(x)$ is an ideal of $\mathcal{O}_K$ admitting a factorization into prime ideals. Write $v_\wp(x)$ as the power of $\wp$ in the ideal-factorization of $(x)$. For any constant $c > 1$, let $|x| = c^{-v_\wp(x)}$ for $x \neq 0$ and $|x| = \infty$.

In the $\wp$-adic valuation, things are "small" when they are divisible by large $\wp$-powers. In the case of number fields $K$, these are the only types of valuations on $K$. The $\wp$-adic valuation allows us to see primes of a field without passing through any rings.

One defines a global field by stating that all valuations on the field have some global coherence, wheras in the case of local fields, we are only looking at one prime, that is only one of the valuations of a local field. We will get to the definition of local fields soon. Let us begin with some examples.

**Example 1.8.** The real numbers $\mathbb{R}$.

**Example 1.9.** The complex numbers $\mathbb{C}$.

**Example 1.10.** Let $p$ be a prime. The $p$-adic numbers $\mathbb{Q}_p$ is a local field.

**Exercise 1.11.** Let $K$ be a number field and $v_\wp$ be the valuation with respect to the prime ideal $\wp$. Let $K_\wp$ be the completion of $K$ with respect to the metric $v_\wp$. $K_\wp$ is a local field.

In this way, local fields only allow us to see one prime of a global field at a time. Note that $\mathbb{R}$ arises as a local field via the completion with respect to a metric, as the completion of $\mathbb{Q}$ with respect to the Euclidean norm.

There are several connections between local and global fields as statements about global fields can sometimes be reduced to statements about global fields such as via local to global principles.

**Theorem 1.12** (Hasse-Minkowski)**.** Let $Q$ be a quadratic form over a number field $K$. The form $Q$ has a non-trivial solution over $K$ if and only if $Q$ has non-trivial solutions over every completion of $K$.

We will study questions like these in the context of local fields. Continuing with our discussion, we can define discrete valuation rings as in [1, §1]. We will continue developing the theory as in this text in the coming semester.

**Definition 1.13** (Discrete Valuation)**.** Let $K$ be a field. The field $K$ is discretely valued if there is a surjective homomorphism $v : K^\times \to \mathbb{Z}$ such that $v(x+y) \geq \min\{v(x), v(y)\}$ and $v(0) = \infty$.

This allows us to define a Discrete Valuation ring, or DVR.

**Definition 1.14** (DVR)**.** Let $K$ be a field with discrete valuation $v$. Let

$$A = \{x \in K | v(x) \geq 0\}$$

is a discrete valuation ring with fraction field $K$.

Let us consider the following examples.

**Example 1.15.** Let $K = \mathbb{Q}$ and $p$ a prime. $A = \mathbb{Z}_{(p)} = \{\frac{r}{s} | p \nmid s; r, s \in \mathbb{Z}\} \subsetneq \mathbb{Q}$ is a DVR.

**Example 1.16.** Let $k$ be a field and $k((t))$ be the field of Laurent series on $k$, that is for some $n_0 > -\infty$, $\sum_{n \geq n_0} a_n t^n$. There is a discrete valuation on the field of Laurent series by

$$v\left(\sum_{n \geq n_0} a_n t^n\right) = n_0.$$

the DVR $A$ here is just the power series on $k$, $k[[t]]$.

**Definition 1.17** (Uniformizer)**.** An element $\pi \in K$ is a uniformizer if $v(\pi) = 1$.

Let us consider the following example.

**Example 1.18.** Let $\mathbb{Q}$ be a field endowed with the $p$-adic valuation. All integers with prime $p$ appearing exactly once in the prime factorization is a uniformizer.

Indeed, for $x \in A \setminus \{0\}$, we can write $x = \pi^n u$ for some $u \in A^\times$. Let $\mathfrak{m} = (\pi) = \pi A$ the ideal generated by $\pi$. We can show $\mathfrak{m} = \{x \in K | v(x) \geq 1\}$ and that $\mathfrak{m}$ is a maximal ideal. We define the residue field to be $A/\mathfrak{m}$.

## 2. Lecture 2 – 13th September 2023

Let us begin by recalling some facts about integrality.

**Definition 2.1** (Integral Domain)**.** A ring $A$ is an integral domain if it has no zerodivisors, that is, there do not exist $a, b \in A \setminus \{0\}$ such that $ab = 0$.

**Definition 2.2** (Integral Over)**.** Let $A, B$ be rings and $A \subseteq B$. An element $x \in B$ is integral over $A$ if it is the root of some monic polynomial with coefficients in $A$. The ring $B$ is integral over $A$ if all its elements are integral over $A$.

**Definition 2.3** (Integrally Closed)**.** A ring $A$ is integrally closed if all elements of the fraction field $K(A)$ are integral over $A$.

Let us consider some examples.

**Example 2.4.** $\mathbb{Z}$ is integrally closed. This is the content of Gauss' lemma.

**Example 2.5.** Let $K$ be a number field and $\mathcal{O}_K$ be its ring of integers. $\mathcal{O}_K$ is integrally closed.

In fact, we can show that DVRs are also integrally closed. To do so, we first show the follwing lemma.

**Lemma 2.6.** Let $A$ be a DVR with fraction field $K(A)$. If $x_1, \ldots, x_n \in K(A)$ are such that $v(x_i) > v(x_1)$ for all $i \geq 2$, then $x_1 + \cdots + x_n \neq 0$.

*Proof.* Suppose to the contrary $x_1 + \cdots + x_n = 0$. Equivalently $x_2 + \cdots + x_n = -x_1$ and applying the valuation we see that $v(x_2 + \cdots + x_n) \geq \min\{v(x_2), \ldots, v(x_n)\} > v(x_1) = v(-x_1)$ a contradiction since $v(x_2 + \cdots + x_n) \neq v(x_1) = v(-x_1)$. ∎

We can now show the desired fact.

**Proposition 2.7** (DVRs Integrally Closed)**.** A DVR $A$ is integrally closed.

*Proof.* Let $x \in K(A)$ such that it satisfies the monic polynomial in $A$

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0.$$

We seek to show $x \in A$, that is, $v(x) \geq 0$. Suppose to the contrary that $v(x) = -m$ for some $m > 0$. Applying the discrete valuation on $A$ to the polynomial, we have $v(x^n) = -mn$ and each of the latter summands have valuations at least $-(n-1)m > -nm = v(x^n)$ since each of the $a_i$ have non-negative discrete valuations. Applying the lemma above, $x$ cannot be the root of the polynomial, giving a contradiction and showing that $v(x) \geq 0$ as desired. ∎

Let us narrow our focus to Dededekind domains and understand these through the eyes of DVRs. To do this, we will first have to define localization.

**Definition 2.8** (Localization)**.** Let $A$ be an integral domain and $K(A)$ its fraction field. Let $S \subseteq A$ be a multiplicatively closed subset of $A$ containing 1. We define the localization of $A$ away from $S$ as the set

$$S^{-1}A = \left\{ \frac{a}{s} | a \in A, s \in S \right\}$$

under the operations of addition and multiplication.

**Example 2.9.** Let $S = A \setminus \{0\}$ then $S^{-1}A = K(A)$, the fraction field of $A$.

**Example 2.10.** Let $S = A^\times$ then $S^{-1}A = A$.

The prime ideals in $A$ and $S^{-1}A$ are closely related in the following way: the prime ideals in $S^{-1}A$ are those prime ideals in $A$ not intersecting $S$.

**Proposition 2.11.** There is a bijection between prime ideals of $A$ and $S^{-1}A$ sending a prime ideal $\wp \subseteq A$ to $\wp S^{-1} = \{\frac{p}{s} | p \in \wp, s \in S\}$ and conversely sending $\wp \subseteq S^{-1}A$ to $\wp \cap A$.

*Proof.* ∎

**Example 2.12.** Let $S = A \setminus \wp$ for $\wp$ a prime ideal. We write $A_\wp = S^{-1}A$ the localization of $A$ away from $\wp$. The ideals of $A_\wp$ are exactly those primes contained in $\wp$ so $A_\wp$ has a unique maximal ideal, that is, $A_\wp$ is a local ring.

Introducing some notation, let $I \subseteq A$ be an ideal. We denote $I_\wp \subseteq A_\wp$ the ideal in $A_\wp$ generated by $I$.

**Theorem 2.13.** Let $A$ be a Noetherian integral domain. The following are equivalent:

(i) For every nonzero prime ideal $\wp \subseteq A$, $A_\wp$ is a DVR.
(ii) $A$ is integrally closed and of Krull dimension at most 1.

This is [1, Ch. 1, §1, Prop. 4].

*Proof.* (i)$\Longrightarrow$(ii)

(ii)$\Longrightarrow$(i) ∎

We use these equivalent conditions to define a Dedekind domain.

**Definition 2.14** (Dedekind Domain)**.** A Dedekind domain is a Noetherian integral domain $A$ that satisfies either of the equivalent conditions in Theorem 2.13.

Some examples of Dedekind domains are as follows.

**Example 2.15.** $\mathbb{Z}, \mathcal{O}_K$ for $K$ a number field, $\mathbb{F}_q[t]$, and $\mathbb{C}[t]$ are all Dedekind domains.

**Example 2.16.** Any PID is a Dedekind domain. Using the fact that PIDs are UFDs, one can yield a valuation by considering factorizations of the ideal generated by an element into prime ideals.

One can also show that the property of being a Dedekind domain is preserved under localization.

**Proposition 2.17.** If $A$ is a Dedekind domain and $S$ a multiplicative subset of $A$, the localization $S^{-1}A$ is a Dedekind domain.

*Proof.* ■

Let $A$ be an integral domain and $K(A)$ its field of fractions. For $x \in K(A)$, we want to assign a valuation to $A$ with respect to some prime ideal $\wp$ of $A$. We make sense of this in terms of fractional ideals which provide a notion of multiplicative inverse for ideals.

**Definition 2.18** (Fractional Ideal)**.** Let $A$ be an integral domain with fraction field $K(A)$. A fractional ideal of $A$ is a finitely generated $A$-submodule of $K(A)$.

Given two $A$-submodules of $K(A)$, we can multiply them

$$IJ = \left\{ \sum_{i=1}^{n} a_i b_i | a_i \in I, b_i \in J \right\}.$$

**Definition 2.19** (Invertible)**.** An ideal $I$ is invertible if there exists $J$ such that $IJ = A$.

In the case of Dedekind domainsm we can show that every ideal is invertible. This is a key part of the proof of the unique factorization property in Dedekind domains, and can in fact be used to define Dedekind domains themselves.

**Proposition 2.20** (Dedekind Ideals are Invertible)**.** Let $A$ be a Dedekind domain. Every nonzero fractional ideal is invertible.

*Proof.* ■

We apply this to the factorization of ideals.

**Theorem 2.21** (Factorization in Dedekind Domains)**.** Let $A$ be a Dedekind domain. Every fractional ideal $I$ can be written uniquely as

$$I = \prod_{\wp_i \text{ prime}} \wp_i^{e_i}$$

only finitely many $e_i$ nonzero.

*Proof.* ■

Returning to integrality, we prove the following statement that we will later use.

**Proposition 2.22.** Let $A \subseteq B$ be rings. The elements $b_1, \ldots, b_n \in B$ are integral over $A$ if and only if $A[b_1, \ldots, b_n]$ is finitely generated as an $A$-module.

Note that $A[b_1, \ldots, b_n]$ is finitely generated as an $A$-algebra, we are asking for something stronger.

*Proof.* ■

## References

[1] Jean-Pierre Serre. *Local fields. Translated from the French by Marvin Jay Greenberg*. English. Vol. 67. Grad. Texts Math. Springer, Cham, 1979.

Bowdoin College, Brunswick, Maine 04011
*Email address*: gong@bowdoin.edu
*URL*: https://wgabrielong.github.io/