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 [2, §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 π. 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. ∎

More explicitly, we can show that the condition in Proposition 2.7 in conjunction with the condition of having a unique nonzero prime ideal to characterize DVRs.

Proposition 2.8. A Noetherian integral domain A is a DVR if and only if it is integrally closed and has a unique nonzero prime ideal.

Proof. See [2, Ch. 1, §2, Prop. 3]. ∎

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

Definition 2.9 (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 2.10. Let $S = A \setminus \{0\}$ then $S^{-1}A = K(A)$, the fraction field of A.

Example 2.11. 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 2.12. There is a bijection between prime ideals of A and $S^{-1}A$ sending a prime ideal $\wp \subseteq A$ to $S^{-1}\wp = \{\frac{p}{s} | p \in \wp, s \in S\}$ and conversely sending $\wp \subseteq S^{-1}A$ to $\wp \cap A$.

Proof. Let $\wp$ be a prime ideal of A not intersecting S and consider $\frac{ab}{s_1 s_2} \in S^{-1}\wp$ where $a, b \in A, s_1, s_2 \in S$. There is $\frac{c}{s} \in S^{-1}\wp$ such that $\frac{ab}{s_1 s_2} = \frac{c}{s}$ or equivalently that for some $t \in S$, we have $t(abs - cs_1 s_2) = 0$ where $abst = cs_1 s_2 t$ and $abst \in \wp$. Noting $st \in S$ with S multiplicatively closed and $S \cap \wp = \emptyset$ $ab \in \wp$ since $\wp$ is prime in A and one of a, b is in $\wp$. So one of $\frac{a}{s_1}, \frac{b}{s_2} \in S^{-1}\wp$. One can also see by definition of $S^{-1}\wp = \{\frac{p}{s} | p \in \wp, s \in S\}$ that $S^{-1}\wp \cap A = \wp$.

Let $\overline{\wp}$ be a prime ideal in $S^{-1}A$. Under the homomomorphism of rings $\varphi : A \to S^{-1}A$, we know $\varphi^{-1}(\overline{\wp}) = \{a \in A | \frac{a}{1} \in \overline{\wp}\} \subseteq A$ is a prime ideal. Suppose to the contrary that $S \cap \wp \neq \emptyset$ then $1 \in \overline{\wp}$ and $\overline{\wp} = S^{-1}A$ contradicting that $\overline{\wp}$ is prime in $S^{-1}A$. One can also see that $S^{-1}\wp = \{\frac{a}{s} | a \in \wp, s \in S\} = \overline{\wp}$ proving the bijective correspondence. ∎

Example 2.13. 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. We will soon prove some equivalent conditions for a Noetherian integral domain to be a Dedekind domain. To do so, we require the following lemma.

Lemma 2.14. Let A be an integral domain. We have an equality $\cap_{\wp \text{ prime}} A_\wp = A$.

Proof. Let $x \in \cap_{\wp \text{ prime}} A_\wp$ and write $x = \frac{a}{b}$. Consider the ideal $\mathfrak{a} \subseteq A$ by $\mathfrak{a} = \{c \in A | ca \in (b) \subseteq A\}$ which can be thought of as the ideal of denominators of x. For every prime $\wp$, $\mathfrak{a} \not\subseteq \wp$ as $x \in A_\wp$ but every proper ideal is contained in some maximal ideal so we have $\mathfrak{a} = A$, showing that $x \in A$. ∎

We can now show the following theorem that we will use to characterize Dedekind domains.

Theorem 2.15. 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 [2, Ch. 1, §1, Prop. 4].

Proof. (i)$\Longrightarrow$(ii) Suppose $\wp \subseteq A$ is a prime ideal and $\mathfrak{m}$ the maximal ideal containing $\wp$. The local ring $A_\mathfrak{m}$ contains the prime ideal $\wp_\mathfrak{m}$ by Proposition 2.12. Since $\mathfrak{m}$ is prime, $A_\mathfrak{m}$ is a DVR by assumption and given that the sole prime ideal in a DVR is (π) for π some uniformizer, we have either $\wp_\mathfrak{m} = (0)$ or $\wp_\mathfrak{m} = (\pi)$ showing that A is of Krull dimension 1. To see that A is integrally closed, note that for some $x \in K(A)$ be integral over A. We want to show that $x \in A$ but $x \in A_\wp$ for all primes $\wp$ so by Lemma 2.14, $x \in A$ showing that A is integrally closed.

(ii)$\Longrightarrow$(i) Suppose that A is integrally closed and of Krull dimension at most 1. Let $\wp \subseteq A$ be a nonzero prime ideal and consider the localization $S^{-1}A$ for $S = A \setminus \wp$. The ring $S^{-1}A$ has a unique nonzero prime ideal $S^{-1}\wp$. By Proposition 2.8, it suffices to show that $S^{-1}A$ is integrally closed. Let $x \in K(S^{-1}A) = K(A)$ be integral over $S^{-1}A$ so it satisfies

$$x^n + b_{n-1}x + \cdots + b_1 x + b_0 = 0 \tag{2.1}$$

for some $b_i \in S^{-1}A$. Writing each $b_i = \frac{a_i}{s_i}$ for $a_i \in A, s_i \in S$, we can take $s = \prod_{i=0}^{n-1} s_i$ and multiply (2.1) by s^n to yield

$$\begin{aligned} 0 &= s^n x^n + a_{n-1}\left(s_{n-1}^{n-1} \prod_{0\le i\le n-2} s_i^n\right) x^{n-1} + \cdots + a_1\left(s_1^{n-1} \prod_{0\le i\le n-1, i\neq 1} s_i^n\right) x + a_0\left(s_0^{n-1} \prod_{1\le i\le 0} s_i^n\right) \\ &= (sn)^n + a_{n-1}\left(\prod_{0\le i\le n-2} s_i\right)(sx)^{n-1} + \cdots + a_1\left(s_1^{n-2} \prod_{0\le i\le n-1, i\neq 1} s_i^{n-1}\right)(sx) + a_0\left(s_0^{n-1} \prod_{1\le i\le 0} s_i^n\right) \end{aligned}$$

wherein $sx \in A$ and each

$$a_{n-1}\left(\prod_{0\le i\le n-2} s_i\right), \ldots, a_1\left(s_1^{n-2} \prod_{0\le i\le n-1, i\neq 1} s_i^{n-1}\right), a_0\left(s_0^{n-1} \prod_{1\le i\le 0} s_i^n\right) \in A.$$

so by A being integrally closed we conclude $sx \in A$ and thus $x \in S^{-1}A$ as desired. ∎

We use these equivalent conditions to define a Dedekind domain.

Definition 2.16 (Dedekind Domain)**.** A Dedekind domain is a Noetherian integral domain A that satisfies any one of the equivalent conditions in Theorem 2.15.

Some examples of Dedekind domains are as follows.

Example 2.17. $\mathbb{Z}, \mathcal{O}_K$ for K a number field, $\mathbb{F}_q[t]$, and $\mathbb{C}[t]$ are all Dedekind domains.

Example 2.18. 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 2.19. If A is a Dedekind domain and S a multiplicative subset of A, the localization $S^{-1}A$ is a Dedekind domain.

Proof. We show condition (b) in Theorem 2.15. By hypothesis A is a Dedekind domain so it is integrally closed and of Krull dimension at most 1. Since prime ideals of $S^{-1}A$ are those of A not meeting S, $S^{-1}A$ is also of Krull dimension at most 1. One then applies the proof in the latter part of Theorem 2.15 to show integral closure. ■

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 2.20 (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 2.21 (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 2.22 (Dedekind Ideals are Invertible)**.** Let A be a Dedekind domain. Every nonzero fractional ideal is invertible.

Proof. Let A be a Dedekind domain and $I \subseteq A$ a fractional ideal. Let $J = \{x \in K | xI \subseteq A\}$. We have $IJ \subseteq A$. Suppose to the contrary that $IJ \subsetneq A$. The ideal IJ is contained in some maximal ideal $\mathfrak{m}$ so localizing at $\mathfrak{m}$ we have $J_\mathfrak{m} = \{x \in K | xI_\mathfrak{m} \in A_\mathfrak{m}\}$, that is, the inverse of $I_\mathfrak{m}$ as fractional ideals of $A_\mathfrak{m}$. In particular, observe $(IJ)_\mathfrak{m} = I_\mathfrak{m} J_\mathfrak{m} = A_\mathfrak{m}$, a contradiction as $IJ \subseteq \mathfrak{m}$. ■

We apply this to the factorization of ideals.

Theorem 2.23 (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.

The proof of uniqueness was given in class. For existence, we adapt the proof from [1, §3, Thm. 14].

Proof. (Existence) Suppose to the contrary that there is some collection of ideals not admitting a decomposition into prime dieals as above. Let $\mathfrak{q}$ be the maximal among such ideals not admitting a decomposition into primes where $\mathfrak{q} \neq A$ as A is the empty product. Let $\mathfrak{p}$ be a prime ideal of A containing $\mathfrak{q}$ and note that $\mathfrak{p} = \mathfrak{q}\mathfrak{a}$ for some ideal $\mathfrak{a} \subseteq A$ since $\mathfrak{q} \subseteq \mathfrak{p}$ implies $\mathfrak{p}|\mathfrak{q}$. But $\mathfrak{a}$ contains $\mathfrak{q}$ so $\mathfrak{q}|\mathfrak{a}$ and in fact $\mathfrak{q} \subsetneq \mathfrak{a}$ as otherwise $\mathfrak{a} = \mathfrak{q}$ and $\mathfrak{q} = \mathfrak{p}\mathfrak{q}$ implying $A = \mathfrak{p}$ a contradiction as $\mathfrak{p}$ was taken to be prime and hence proper. Using $\mathfrak{q} \subsetneq \mathfrak{a}$ we have $\mathfrak{a}$ is a product of primes and so is $\mathfrak{q}$, a contradiction.

(Uniqueness) Let $I \subseteq A$ be an ideal admitting a decomposition by

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

For each $\wp_i$, $I_{\wp_i}$ is an ideal in the DVR $A_{\wp_i}$ and $e_i = v_{\wp_i}(x)$ for x a generator of $I_{\wp_i}$ in $A_{\wp_i}$. ∎

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

Proposition 2.24. 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. ($\Longrightarrow$) By induction, it suffices to show that if $b \in B$ is integral over A the ring $A[b]$ is finitely generated as an A-module. Suppose $b \in B$ is integral over A so

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

for some $a_0, a_1, \ldots, a_{n-1} \in A$. Thus $A[b]$ is generated by $1, b, \ldots, b^{n-1}$ as an A-module, that is, finitely generated as an A-module.

($\Longleftarrow$) Suppose $w_1, \ldots, w_m$ generate $A[b_1, \ldots, b_n]$ as an A-module. For $b \in A[b_1, \ldots, b_n]$ and any w_i we can write

$$bw_i = \sum_{j=1}^{m} a_{ij} w_j$$

with $a_{ij} \in A$. We use this A-linear expression to construct an integral dependence polynomial. Let

$$M = \begin{bmatrix} b - a_{11} & -a_{12} & \ldots & -a_{1m} \\ -a_{21} & b - a_{22} & \ldots & a_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ -a_{m1} & -a_{m2} & \ldots & b - a_{mm} \end{bmatrix}.$$

Observe that

$$M \begin{bmatrix} w_1 \\ \vdots \\ w_m \end{bmatrix} = 0_m$$

so for M^* the adjoint matrix satisfying $M^*M = \det M I_m$ we can consider the equation

$$M^*M \begin{bmatrix} w_1 \\ \vdots \\ w_m \end{bmatrix} = \det M \begin{bmatrix} w_1 \\ \vdots \\ w_m \end{bmatrix} = 0_m$$

as 1 can be written as a linear cobmination of the w_is. Thus $\det M$ is a monic in A satisfied by $b \in A[b_1, \ldots, b_n]$ showing that $A[b_1, \ldots, b_n]$ is integral over A. ∎

3. Lecture 3 – 18th September 2023

Let us recall Proposition 2.24 with which we ended the previous lecture.

Proposition 3.1 (=Proposition 2.24)**.** 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.

One can deduce the following corollaries.

Corollary 3.2. Let $A \subseteq B$ be rings. The elements of B integral over A form a subring of B.

Proof. If $b_1, b_2 \in B$ are integral over A then $b_1 b_2, b_1 + b_2 \in A[b_1, b_2]$. ∎

Corollary 3.3. Let $A \subseteq B \subseteq C$ be a tower of rings. If B is integral over A and C is integral over B then C is integral over A.

Proof. If c_i generate C over B and the b_j generate B over A then the $c_i b_j$ generate C over A. ∎

We now turn to extensions of Dedekind domains. More precisely, let A be a Dedekind domain and K its fraction field. Let B be the integral closure of A in L.

$$\begin{array}{ccc} B & \hookrightarrow & L \\ \downarrow & & \downarrow \\ A & \hookrightarrow & K \end{array}$$

Let us consdier some examples from the number field and function field case.

Example 3.4. For a cubic extension of fields $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$, both $\mathbb{Z}$ and $\mathbb{Z}[\sqrt[3]{2}]$ are Dedekind domains.

$$\begin{array}{ccc} \mathbb{Z}[\sqrt[3]{2}] & \hookrightarrow & \mathbb{Q}(\sqrt[3]{2}) \\ \downarrow & & \downarrow \\ \mathbb{Z} & \hookrightarrow & \mathbb{Q} \end{array}$$

Example 3.5. Fix some finite field $\mathbb{F}_q$ of characteristic not 2. Let $A = \mathbb{F}_q[t]$ with field of fractions $K = \mathbb{F}_q(t)$. Let

$$L = \mathbb{F}_q(t)[\sqrt{t^3 + t + 1}] = \mathbb{F}_q(t)[s]/(s^2 - t^3 - t - 1).$$

One can verify that $[L : K] = 2$ where K are the functions on $\mathbb{P}^1_{\mathbb{F}_q}$ and L are the functions on the elliptic curve $s^2 = t^3 + t + 1$ (more often written $y^2 = x^3 + x + 1$) and the extension of fields L/K corresponds to the 2-1 map $E \to \mathbb{P}^1_{\mathbb{F}_q}$ from the elliptic curve to the projective line. The integral closure of L in $A = \mathbb{F}_q[t]$ is $B = \mathbb{F}_q[t][\sqrt{t^3 + t + 1}]$.

Remark. One could also take $A = \mathbb{F}_q[\frac{1}{t}]$ and the same extensions L/K. But now $\sqrt{t^3 + t + 1}$ is no longer integral over A.

Proposition 3.6. If A is a Dedekind domain with fraction field K and B the integral closure of A in L for L/K a finite extention of fields, the ring B is an integral domain with fraction field L.

Proof. The integral closure of A in L is a subring by Corollary 3.2. It remains to show that B has fraction field L. ∎

We want to show a stronger fact, that B is in fact itself a Dedekind domain. This parallels what we have seen before. For K a number field and L/K a finite extension of fields, $\mathcal{O}_L$ is also a Dedekind domain. We are seeking a proof that generalizes appropriately to non-separable extensions and the function field case. In this setting, we lose nice properties such as separability. But first, let us return to the simpler case of separable extensions.

To consider this case, we recall some notions from our first course in algebraic number theory. For an extension of fields L/K, multiplication by an element $x \in L$ gives a linear transformation of K-vector spaces $m_x : L \to L$ by $\alpha \mapsto x\alpha$. The linear transformation admits a trace which we denote $\mathrm{Tr}_{L/K}(x) = \mathrm{tr}(m_x)$ and a norm $\mathrm{Nm}_{L/K}(x) = \det(m_x)$. If further L/K is a Galois extension, we can compute $\mathrm{Tr}_{L/K}(x) = \sum_{\sigma \in \mathrm{Gal}(L/K)} \sigma(x)$ and $\mathrm{Nm}_{L/K}(x) = \prod_{\sigma \in \mathrm{Gal}(L/K)} \sigma(x)$. Finally, recall that the K-bilinear form $\langle x, y\rangle = \mathrm{Tr}_{L/K}(xy)$ is nondegenerate if and only if L/K is separable – a bilinear form is nondegenerate if $\langle x, y\rangle = 0$ for all y then $x = 0$. We can now prove the following.

Proposition 3.7. Let A be a Dedekind domain with fraction field K and B the integral closure of A in L for L/K a finite extention of fields. If further L/K is separable, the ring B is a finitely generated A-module (i.e. satisfies Serre's "Hypothesis F").

This is [2, Ch. 1, §4, Prop. 8].

Proof. For $x \in B$ we know it is integral over A by hypothesis so $\mathrm{Tr}_{L/K}(x) \in A$ as it is an integral multiple of the coefficient of x by [3, 0BIH]. Let $\{e_i\}$ be a basis of L over K. Without loss of generality, we can take $\{e_i\} \subseteq B$ by clearing denominators. Let V be the free A-module spanned by the $\{e_i\}$. Using the trace map, we consider the dual module

$$V^* = \left\{x \in L | \mathrm{Tr}_{L/K}(xy) \in A, \forall y \in V\right\}.$$

We have $V \subseteq B$ by inspection as the $\{e_i\}$ were chosen in B and $B^* \subseteq V^*$ where V^* is the free module spanned by the basis dual to $\{e_i\}$ with respect to the trace bilinear form the existence of which is given by separability. In particular, B is an A-submodule of V^* which was finitely generated by the finite dual basis. ∎

To show that integral closures of Dedekind domains are Dedekind domains, however, will require some lemmata, some of which was assigned as homework.

Lemma 3.8. If $\wp \subseteq \wp'$ are prime ideals of B and $\wp \cap A = \wp' \cap A$ then $\wp = \wp'$.

Proof. Consider the quotient $B/\wp$ and for $x \in \wp' \setminus \wp$ its image $\overline{x} \in B/\wp$. Quotients are homomorphisms of rings so

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

and rearranging we see that $a_0 \in (\overline{x}) \subseteq \overline{A}$, that is, $a_0 \in \overline{\wp' \cap A}$ but not $\overline{\wp \cap A}$ a contradiction. ∎

Lemma 3.9. In a 0-dimensional Noetherian ring, any descending chain of ideals stabilizes.

Lemma 3.10. Let A be a Dedekind domain with fraction field K and B the integral closure of A in L for L/K a finite extension of fields. Let $w_1, \ldots, w_n \in L$ be an L-basis fully contained in B and denote $B_0 = A[w_1, \ldots, w_n]$. If $a \in A$ then B_0/aB_0 is a 0-dimensional Noetherian ring.

Granting the lemmata, we can prove the theorem.

Theorem 3.11. Let A be a Dedekind domain with fraction field K and B the integral closure of A in L for L/K a finite extension of fields. The ring B is a Dedekind domain.

Proof. We seek to show that B is Noetherian, integrally closed and of Krull dimension 1. By construction, B is integrally closed. Suppose to the contrary that B is of Krull dimension more than 1 and we have a strict chain of prime ideals $\wp_1 \subsetneq \wp_2 \subsetneq_3$ of B. Contraposing Lemma 3.8 and intersecting down to A we have $\wp_1 \cap A \subsetneq \wp_2 \cap A \subsetneq \wp_3 \cap A$, a contradiction as A was Dedekind by assumption and of Krull dimension at most 1.

It remains to show B is Noetherian. Let $w_1, \ldots, w_n$ be a K-basis of L contained in B with each w_i integral over A and let $B_0 = A[w_1, \ldots, w_n]$. By Proposition 2.24, B_0 is a finitely generated A-module and therefore Noetherian. To show B is itself Noetherian, we will show that any ideal $I \subseteq B$ is a finitely generated B-module for nonzero ideals I. We claim that for $a \in I \cap A$, B/aB is a finitely generated B-module. Granting Lemma 3.10, consider the decreasing sequence of ideals in B_0 given by $(a^m B \cap B_0, aB_0)$ for $m \geq 1$ which correspond to a descending sequence $\overline{(a^m B \cap B_0)}$ in B_0/aB_0. By Lemma 3.10, they stabilize at some $m \geq n$. For $\beta \in B$, we want to show that $\beta \in a^{-n}B_0 + aB$. Take h minimal such that β can be expressed as $a^{-h}B_0 + aB$. If $h \leq n$ we are done. Otherwise suppose to the contrary that $h > n$. Let $\beta = \frac{u}{a^h} + a\widetilde{u}$ for $u \in B_0, \widetilde{u} \in B$. Rearranging this expression, we have $a^h(\beta - a\widetilde{u})$ so $u \in a^h B \cap B_0$ which lies in I_h but $h > n$ contradicting the stabilization if ideals so $u \in I_h = I_{h-1}$ so $a^{h-1}\widetilde{u'} + au'$ so $u' \in B_0, \widetilde{u'} \in B$ so $\beta = \frac{u'}{a^{h-1}} + a(\widetilde{u} + \widetilde{u'})$ contradicting minimality of h. So $B/aB \subseteq (a^{-n}B_0 \cap aB)/aB$ and B/aB is a finitely generated B_0-module. Then B/aB is a finitely generated A module and for an ideal I containing aB of B, I/aB is a finitely genereated A-module in B/aB with A Noetherian, so I is a finitely generated B-module. ∎

4. Lecture 4 – 20th September 2023

We continue our discussion of extensions of Dedekind domains. Let us recall the setup. Let A be a Dedekind domain with fraction field K and B the integral closure of A in L, where L/K is a finite extension of fields. By Theorem 3.11, B is a Dedekind domain. Let $\mathfrak{p}$ be a nonzero prime ideal of A. Write $\wp = \mathfrak{p}B$ be its "lift" in B. Since B is Dedekind, $\wp$ admits a unique factorization into prime ideals $\prod_i \wp_i^{e_i}$ finitely many e_i nonzero. In such a setting, we write $\wp_i | \mathfrak{p}$.

Definition 4.1 (Ramifies)**.** Let $\mathfrak{p} \subseteq A$ be an ideal and $\mathfrak{p}B = \prod_i \wp_i^{e_i}$ with finitely many e_i nonzero. If $e_i \geq 1$, the ideal $\wp_i \subseteq B$ ramifies with ramification index e_i in L/K. Similarly if $e_i \geq 1$ and $\wp_i | \mathfrak{p}$ for $\mathfrak{p} \subseteq A$ then $\mathfrak{p}$ ramifies in A.

Proposition 4.2. If $\mathfrak{p} \subseteq A$ is an ideal and $\mathfrak{p}B = \prod_i \wp_i^{e_i}$ with finitely many e_i nonzero then $\wp_i \cap A = \mathfrak{p}$.

Proof. We have an injective map of rings $A/(\wp_i \cap A) \to B/\wp_i$ where $B/\wp_i$ is integral as $\wp_i$ is prime so we have $\mathfrak{p} \subseteq \mathfrak{p}B \cap A \subseteq \wp_i \cap A$ but since $\mathfrak{p}$ is nonzero, $\mathfrak{p} = \wp_i \cap A$ as desired. ∎

Definition 4.3 (Inertia Degree)**.** Let $\mathfrak{p} \subseteq A$ be a nonzero ideal and $\mathfrak{p}B = \prod_i \wp_i^{e_i}$ with finitely many e_i nonzero with $\mathfrak{p}, \wp_i$ maximal. We define the inertia degree of $\wp_i$ in L/K by $f_{\wp_i} = [B/\wp_i : A/\mathfrak{p}]$.

Definition 4.4 (Split Completely)**.** Let $\mathfrak{p} \subseteq A$ be a nonzero ideal and $\mathfrak{p}B = \prod_i \wp_i^{e_i}$ with finitely many e_i nonzero with $\mathfrak{p}, \wp_i$ maximal. The ideal $\mathfrak{p}$ is split completely if $e_i = f_{\wp_i} = 1$ for all $\wp_i$.

Inertia and ramification degrees are connected in the following way:

Proposition 4.5. Let $\mathfrak{p} \subseteq A$ be a nonzero ideal and $\mathfrak{p}B = \prod_i \wp_i^{e_i}$ with finitely many e_i nonzero. Under the conditions of Serre's Hypothesis F, where B is a finitely generated A-module, $[L : K] = \sum_{\wp_i} e_i f_{\wp_i}$.

Proof. This is [2, Ch. 1, §4, Proposition 10]. ∎

Note that without Serre's Hypothesis F, we only have the inequality $[L:K] \geq \sum_{\wp_i} e_i f_{\wp_i}$.

For A a Dedekind domain, the set of fractional ideals of A forms a group in a natural way which we denote I_A. For B the integral closure of A, we can define a map $I_B \to I_A$ using the relative ideal norm as follows.

Definition 4.6 (Relative Ideal Norm)**.** Let $A \subseteq B$ be Dedekind domains. The relative ideal norm $\mathrm{Nm}_{B/A} : I_B \to I_A$ is defined by $\wp \mapsto (\wp \cap A)^{f_\wp}$.

The relative ideal norm and the norm on elements are related in the following way.

Proposition 4.7. If $x \in L$ then $\mathrm{Nm}_{B/A}(xB) = \mathrm{Nm}_{L/K}(x)A$.

If further L/K is a Galois extension, there is an action by $\mathrm{Gal}(L/K)$ on the primes $\wp_i \subseteq B$ over $\mathfrak{p} \subseteq A$.

Proposition 4.8. Let A be a Dedekind domain with fraction field K, L/K a Galois extension of field with B the integral closure of A in L, and $\mathfrak{p} \subseteq A$ nonzero. The Galois group $\mathrm{Gal}(L/K)$ acts transitively on $\wp \subseteq B$ for $\wp|\mathfrak{p}$.

Proof. Let $\wp|\mathfrak{p}, \wp'|\mathfrak{p}$ and suppose $\wp, \wp'$ do not lie in the same Galois orbit. Applying the Chinese remainder theorem, we can find $b \in \wp$ scu that $b \notin \sigma(\wp')$, that is, b does not lie in any Galois orbit of $\wp'$. We thus have $\sigma^{-1}(b) \notin \wp$ for any $\sigma \in \mathrm{Gal}(L/K)$. So on one hand $\mathrm{Nm}_{L/K}(b) \in \wp$ and computing by $\mathrm{Nm}_{L/K}(b) = \prod_{\sigma \in \mathrm{Gal}(L/K)} \sigma^{-1}(b)$ is not in $\wp'$ contradicting $\wp' \cap A = \wp \cap A$. ∎

One then deduces the following corollary.

Corollary 4.9. In the setting of Proposition 4.8, $e_i = e_j$ and $f_{\wp_i} = f_{\wp_j}$.

We now introduce two important subgroups of the Galois group of L/K, the decomposition group and the inertia group. These groups allow us to better understand the Galois group as a whole.

Definition 4.10 (Decomposition Group)**.** Let $\wp|\mathfrak{p}$ for $\mathfrak{p} \subseteq A, \wp \subseteq B$ nonzero. The decomposition group of $\wp$ denoted $D_\wp$ is the subgroup of the Galois group $\mathrm{Gal}(L/K)$ stabilizing $\wp$.

By Proposition 4.8 and our first course in the theory of groups $D_\wp$ and $D_{\wp'}$ are conjugate subgroups of $\mathrm{Gal}(L/K)$. Conversely, if $D_\wp, D_{\wp'}$ are conjugate subgroups of $\mathrm{Gal}(L/K)$, then they are decomposition groups for ideals $\wp|\mathfrak{p}, \wp'|\mathfrak{p}$. So each $\mathfrak{p} \subseteq A$ determines a conjugacy class of subgroups of $\mathrm{Gal}(L/K)$ which correspond to decomposition groups of ideals $\wp|\mathfrak{p}$. By the orbit-stabilizer theorem $|D| = ef = \frac{n}{r}$ where $n = [L:K]$ and r is the number of primes of B lying over $\mathfrak{p} \subseteq A$. Note that given a decomposition group D, we can consider the subfield of L fixed by D which we denote K_D where $K \subseteq K_D \subseteq L$. One applies the orbit-stabilizer theorem once again to see that $[K_D : K] = r, [L : K_D] = ef$. Furthermore, one can show that all factorizations of $\mathfrak{p}$ into distinct primes occurs in K_D.

If $A/\mathfrak{p}$ is finite (which holds for our cases of interest), the decomposition group D acts on $B/\wp$ fixing $A/\mathfrak{p}$ inducing a map $\phi : D \to \mathrm{Gal}((B/\wp)/(A/\mathfrak{p}))$. We define the kernel of this map to be the inertia group.

Definition 4.11 (Inertia Group)**.** Let $\wp|\mathfrak{p}$ for $\mathfrak{p} \subseteq A, \wp \subseteq B$ nonzero with$A/\mathfrak{p}$ finite and $D_\wp$ the decomposition group of $\wp$. The inertia group of $\wp$ denoted $T_\wp$ is the kernel of the map $\phi : D \to \mathrm{Gal}((B/\wp)/(A/\mathfrak{p}))$.

The inertia group is the set of elements of D that fix $B/\wp$ pointwise. We can think of it as the set of things that $B/\wp$ cannot see. As in the case of the decomposition group, we can define a field K_T the subfield of L fixed by the inertia group T.

Proposition 4.12. Let $\wp|\mathfrak{p}$ for $\mathfrak{p} \subseteq A, \wp \subseteq B$ nonzero with $A/\mathfrak{p}$ finite, $D_\wp$ the decomposition group of $\wp$, and $T_\wp$ the inertia group of $\wp$. The map $D_\wp/T_\wp \to \mathrm{Gal}((B/\wp)/(A/\mathfrak{p}))$ is an isomorphism.

Proof Outline. By the first isomorphism theorem for groups, it suffices to show that $\phi : D \to \mathrm{Gal}((B/\wp)/(A/\mathfrak{p}))$ is surjective. We can find an element $\sigma \in \mathrm{Gal}(L/K)$ mapping an element to each conjugate by comparing minimal polynomials of elements in B and $B/\wp$. ■

From Proposition 4.12, we see that $|T| = e$.

Remark. The inertia group T is a misleading name as it controls the ramification of primes. This is the first example of the higher ramification groups that we will see later in the course. Moreover, under the assumptions above, we are considering a finite field extension over a finite field, which is well understood.

Proposition 4.13. Let L/K be a Galois extension. If L/K is unramified at $\wp \subseteq B$, then $D = \mathrm{Gal}((B/\wp)/(A/\mathfrak{p}))$ and D is generated by the Frobenius element $\mathrm{Frob}_\wp \in D$ where $\mathrm{Frob}_\wp : B/\wp \to B/\wp$ by $x \mapsto x^{|A/\mathfrak{p}|}$.

We will often use the actions of these groups on L/K and $B/\wp, A/\mathfrak{p}$ in our study of local fields.

Example 4.14. Let $A = \mathbb{Z}, K = \mathbb{Q}, L = \mathbb{Q}(\zeta_n)$ where ζ_n is a primitive n-th root of unity. Recall here that $\mathrm{Gal}(L/K) \cong (\mathbb{Z}/n\mathbb{Z})^\times$ where the isomorphism is by $u \mapsto \zeta_n^u$. One can check using discriminants that if $p \nmid n$ a positive prime, it is unramified and Frob_p is the image of p in the map $(\mathbb{Z}/n\mathbb{Z})^\times \to \mathrm{Gal}(L/K)$. Indeed, infinitely many p in each least residue class $(\mathbb{Z}/n\mathbb{Z})^\times$ Frob_p generates the Galois group.

Remark. The order of the Frobenius element $\mathrm{Frob}_\wp$ is $f_\wp$.

In the setting of non-Galois extensions, we can take the Galois closure and use these groups in the ways we described above.

Proposition 4.15 (=[2, Ch. 1, §7, Prop. 22])**.** Suppose we have a tower of field with their integral closures

$$\begin{array}{ccc} C & \hookrightarrow & M \\ \uparrow & & \uparrow \\ B & \hookrightarrow & L \\ \uparrow & & \uparrow \\ A & \hookrightarrow & K \end{array}$$

we have $D_\wp(M/L) = D_\wp(M/K) \cap \mathrm{Gal}(M/L)$ and $T_\wp(M/L) = T_\wp(M/K) \cap \mathrm{Gal}(M/L)$ for $p \subseteq A, \mathfrak{p} \subseteq B, \wp \subseteq C$ and $\wp|\mathfrak{p}, \mathfrak{p}|p$.

References

[1] Daniel A. Marcus. *Number fields*. English. 2nd edition. Universitext. Cham: Springer, 2018. ISBN: 978-3-319-90232-6; 978-3-319-90233-3. DOI: 10.1007/978-3-319-90233-3.

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

[3] The Stacks project authors. *The Stacks project*. https://stacks.math.columbia.edu. 2023.

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