1 Absolute values and discrete valuations

1.1 Introduction

At its core, number theory is the study of the integer ring $\mathbb{Z}$. By the fundamental theorem of arithmetic, every element of $\mathbb{Z}$ can be written uniquely as a product of primes (up to multiplication by a unit ± 1), so it is natural to focus on the prime elements of $\mathbb{Z}$. If p is a prime, the ideal $(p) := p\mathbb{Z}$ it generates is a maximal ideal ($\mathbb{Z}$ has Krull dimension one), and the residue field $\mathbb{Z}/p\mathbb{Z}$ is the finite field $\mathbb{F}_p$ with p elements (unique up to isomorphism). The fraction field of $\mathbb{Z}$ is the field $\mathbb{Q}$ of rational numbers. The field $\mathbb{Q}$ and the finite fields $\mathbb{F}_p$ together make up the prime fields: every field k contains exactly one of them, according to its characteristic: k has characteristic zero if and only if it contains $\mathbb{Q}$, and k has characteristic p if and only if k contains $\mathbb{F}_p$.

The structure of the ring $\mathbb{Z}$ and the distribution of its primes are both intimately related to properties of the Riemann zeta function

$$\zeta(s) = \sum n^{-s} = \prod_p (1 - p^{-s})^{-1}.$$

As a function of the complex variable s, the Riemann zeta function is holomorphic and nonvanishing on $\operatorname{Re}(s) > 1$ and admits an analytic continuation to the entire complex plane. It has a simple pole at $s = 1$, which implies that there are infinitely many primes (otherwise the product over primes on the RHS would be finite and converge). The distribution of its zeros in the *critical strip* $0 < s < 1$ is directly related to the distribution of primes (via the *explicit formula*, which we will see later in the course). As you are probably aware, Riemann famously conjectured more than 150 years ago that the zeros of $\zeta(s)$ in the critical strip all lie on the *critical line* $\operatorname{Re}(s) = \frac{1}{2}$; this conjecture remains open.

One can also consider finite extensions of $\mathbb{Q}$, such as the field $\mathbb{Q}(i) := \mathbb{Q}[x]/(x^2 + 1)$. These are called *number fields*, and each can be constructed as the quotient of the polynomial ring $\mathbb{Q}[x]$ by one of its maximal ideals; the ring $\mathbb{Q}[x]$ is a principal ideal domain and its maximal ideals can all be written as (f) for some monic irreducible $f \in \mathbb{Z}[x]$. Associated to each number field K is a zeta function $\zeta_K(s)$, and each of these has an associated conjecture regarding the location of its zeros (these conjectures all remain open).

Number fields are one of two types of *global fields* that we will spend much of the course studying; the other type are known as *global function fields*. Let $\mathbb{F}_q$ denote the field with q elements, where q is any prime power. The polynomial ring $\mathbb{F}_q[t]$ has much in common with the integer ring $\mathbb{Z}$. Like $\mathbb{Z}$, it is a principal ideal domain of dimension one, and the residue fields $\mathbb{F}_q[t]/(f)$ one obtains by taking the quotient by a maximal ideal (f), where $f \in \mathbb{F}_q[t]$ is any irreducible polynomial, are finite fields $\mathbb{F}_{q^d}$, where d is the degree of f. In contrast to the situation with $\mathbb{Z}$, the residue fields of $\mathbb{F}_q[t]$ all have the same characteristic as its fraction field $\mathbb{F}_q(t)$, which plays a role analogous to $\mathbb{Q}$. Global function fields are finite extensions of $\mathbb{F}_q(t)$ (this includes $\mathbb{F}_q(t)$ itself, an extension of degree 1).

Associated to each global field k is an infinite collection of *local fields* corresponding to the completions of k with respect to its absolute values; when $k = \mathbb{Q}$, these completions are the field of real numbers $\mathbb{R}$ and the p-adic fields $\mathbb{Q}_p$ (as you will prove on Problem Set 1).

The ring $\mathbb{Z}$ is a principal ideal domain (PID), as is $\mathbb{F}_q[t]$, and in such fields every nonzero prime ideal is maximal and thus has an associated *residue field.* For both $\mathbb{Z}$ and $\mathbb{F}_q[t]$ these residue fields are finite, but the characteristics of the residue fields of $\mathbb{Z}$ are all different (and distinct from the characteristic of its fraction field), while those of $\mathbb{F}_q[t]$ are all the same.

We will spend the first part of this course fleshing out this picture, in which we are particularly interested in understanding the integral closure of the rings $\mathbb{Z}$ and $\mathbb{F}_q[t]$ in finite extensions of their fraction fields (such integral closures are known as *rings of integers*), and the prime ideals of these rings. Where possible we will treat number fields and function fields on an equal footing, but we will also note some key differences. Surprisingly, the apparently more complicated function field setting often turns out to be simpler than the number field setting; for example, the analog of the Riemann hypothesis in the function field setting (the Riemann hypothesis for curves), is not an open problem. It was proved by André Weil in the 1940s [5]; a further generalization to varieties of arbitrary dimension was proved by Pierre Deligne in the 1970s [3].

Zeta functions provide the tool we need to understand the distribution of primes, both in general, and within particular residue classes; the proofs of the prime number theorem and Dirichlet's theorem on primes in arithmetic progressions both use zeta functions in an essential way. Dirichlet's theorem states that for each integer $m > 1$ and each integer a coprime to m, there are infinitely many primes $p \equiv a \bmod m$. In fact, more is true: the Chebotarev density theorem tells us that for each modulus m the primes are equidistributed among the residue classes of the integers a coprime to m. We will see this and several other applications of the Chebotarev density theorem in the later part of the course.

Before we begin, let us note the following.

Remark 1.1. Our rings always have a multiplicative identity that is preserved by ring homomorphisms (so the zero ring in which $1 = 0$ is not an initial object in the category of rings, but it is the terminal object in this category). Except where noted otherwise, the rings we shall consider are all commutative.

1.2 Absolute values

We begin with the general notion of an absolute value on a field; a reference for much of this material is [4, Chapter 1].

Definition 1.2. An *absolute value* on a field k is a map $|\ |\colon k \to \mathbb{R}_{\geq 0}$ such that for all $x, y \in k$ the following hold:

1. $|x| = 0$ if and only if $x = 0$;
2. $|xy| = |x||y|$;
3. $|x + y| \leq |x| + |y|$.

If the stronger condition

4. $|x + y| \leq \max(|x|, |y|)$

also holds, then the absolute value is *nonarchimedean*; otherwise it is *archimedean*.

Example 1.3. The map $|\ |\colon k \to \mathbb{R}_{\geq 0}$ defined by

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

is the *trivial absolute value* on k. It is nonarchimedean.

Lemma 1.4. *An absolute value $|\ |$ on a field k is nonarchimedean if and only if*

$$|\underbrace{1+\cdots+1}_{n}| \le 1$$

for all $n \ge 1$.

Proof. See Problem Set 1. □

Corollary 1.5. *In a field of positive characteristic every absolute value is nonarchimedean, and the only absolute value on a finite field is the trivial one.*

Definition 1.6. Two absolute values $|\ |$ and $|\ |'$ on the same field k are *equivalent* if there exists an $\alpha \in \mathbb{R}_{>0}$ for which $|x|' = |x|^\alpha$ for all $x \in k$.

1.3 Absolute values on $\mathbb{Q}$

To avoid confusion we will denote the usual absolute value on $\mathbb{Q}$ (inherited from $\mathbb{R}$) by $|\ |_\infty$; it is an archimedean absolute value. But there are are infinitely many others. Recall that any element of $\mathbb{Q}^\times$ may be written as $\pm\prod_q q^{e_q}$, where the product ranges over primes and the exponents $e_q \in \mathbb{Z}$ are uniquely determined (as is the sign).

Definition 1.7. For a prime p the *p-adic valuation* $v_p\colon \mathbb{Q} \to \mathbb{Z}$ is defined by

$$v_p\left(\pm\prod_q q^{e_q}\right) := e_p,$$

and we define $v_p(0) := \infty$. The *p-adic absolute value* on $\mathbb{Q}$ is defined by

$$|x|_p := p^{-v_p(x)},$$

where $|0|_p = p^{-\infty}$ is understood to be 0.

Theorem 1.8 (Ostrowski's Theorem). *Every nontrivial absolute value on $\mathbb{Q}$ is equivalent to $|\ |_p$ for some $p \le \infty$.*

Proof. See Problem Set 1. □

Theorem 1.9 (Product Formula). *For every $x \in \mathbb{Q}^\times$ we have*

$$\prod_{p\le\infty} |x|_p = 1.$$

Proof. See Problem Set 1. □

1.4 Discrete valuations

Definition 1.10. A *valuation* on a field k is a group homomorphism $k^\times \to \mathbb{R}$ such that for all $x, y \in k$ we have

$$v(x+y) \ge \min(v(x), v(y)).$$

We may extend v to a map $k \to \mathbb{R}\cup\{\infty\}$ by defining $v(0) := \infty$. For any any $0 < c < 1$, defining $|x|_v := c^{v(x)}$ yields a nonarchimedean absolute value. The image of v in $\mathbb{R}$ is the *value group* of v. We say that v is a *discrete valuation* if its value group is equal to $\mathbb{Z}$ (every discrete subgroup of $\mathbb{R}$ is isomorphic to $\mathbb{Z}$, so we can always rescale a valuation with a discrete value group so that this holds). Given a field k with valuation v, the set

$$A \coloneqq \{x \in k : v(x) \geq 0\},$$

is the *valuation ring* of k (with respect to v). A *discrete valuation ring* (DVR) is an integral domain that is the valuation ring of its fraction field with respect to a discrete valuation; such a ring A cannot be a field, since $v(\operatorname{Frac} A) = \mathbb{Z} \neq \mathbb{Z}_{\geq 0} = v(A)$.

It is easy to verify that every valuation ring A is a in fact a ring, and even an integral domain (if x and y are nonzero then $v(xy) = v(x) + v(y) \neq \infty$, so $xy \neq 0$), with k as its fraction field. Notice that for any $x \in k^\times$ we have $v(1/x) = v(1) - v(x) = -v(x)$, so at least one of x and $1/x$ has nonnegative valuation and lies in A. It follows that $x \in A$ is invertible (in A) if and only if $v(x) = 0$, hence the unit group of A is

$$A^\times = \{x \in k : v(x) = 0\},$$

We can partition the nonzero elements of k according to the sign of their valuation. Elements with valuation zero are units in A, elements with positive valuation are non-units in A, and elements with negative valuation do not lie in A, but their multiplicative inverses are non-units in A. This leads to a more general notion of a valuation ring.

Definition 1.11. A *valuation ring* is an integral domain A with fraction field k with the property that for every $x \in k$, either $x \in A$ or $x^{-1} \in A$.

Let us now suppose that the integral domain A is the valuation ring of its fraction field with respect to some discrete valuation v (which we shall see is uniquely determined). Any element $\pi \in A$ for which $v(\pi) = 1$ is called a *uniformizer.* Uniformizers exist, since $v(A) = \mathbb{Z}_{\geq 0}$. If we fix a uniformizer π, every $x \in k^\times$ can be written uniquely as

$$x = u\pi^n$$

where $n = v(x)$ and $u = x/\pi^n \in A^\times$ and uniquely determined. It follows that A is a unique factorization domain (UFD), and in fact A is a principal ideal domain (PID). Indeed, every nonzero ideal of A is equal to

$$(\pi^n) = \{a \in A : v(a) \geq n\},$$

for some integer $n \geq 0$. Moreover, the ideal (π^n) depends only on n, not the choice of uniformizer π: if π' is any other uniformizer its unique representation $\pi' = u\pi^1$ differs from π only by a unit. The ideals of A are thus totally ordered, and the ideal

$$\mathfrak{m} = (\pi) = \{a \in A : v(a) > 0\}$$

is the unique maximal ideal of A (and also the only nonzero prime ideal of A).

Definition 1.12. A *local ring* is a commutative ring with a unique maximal ideal.

Definition 1.13. The *residue field* of a local ring A with maximal ideal $\mathfrak{m}$ is the field $A/\mathfrak{m}$.

We can now see how to determine the valuation v corresponding to a discrete valuation ring A. Given a discrete valuation ring A with unique maximal ideal $\mathfrak{m}$, we may define $v\colon A \to \mathbb{Z}$ by letting $v(a)$ be the unique integer n for which $(a) = \mathfrak{m}^n$ and $v(0) := \infty$. Extending v to the fraction field k of A via $v(a/b) := v(a) - v(b)$ gives a discrete valuation v on k for which $A = \{x \in k : v(x) \geq 0\}$ is the corresponding valuation ring.

Notice that any discrete valuation v on k with A as its valuation ring must satisfy $v(\pi) = 1$ for some $\pi \in \mathfrak{m}$ (otherwise $v(k) \neq \mathbb{Z}$), and we then have $v(\pi) = 1$ if and only if $\mathfrak{m} = (\pi)$. Moreover, v must then coincide with the discrete valuation we just defined: for any DVR A, the discrete valuation on the fraction field of A that yields A as its valuation ring is uniquely determined. It follows that we could have defined a uniformizer to be any generator of the maximal ideal of A without reference to a valuation.

Example 1.14. For the p-adic valuation $v_p\colon \mathbb{Q} \to \mathbb{Z} \cup \{\infty\}$ we have the valuation ring

$$\mathbb{Z}_{(p)} := \left\{ \frac{a}{b} : a, b \in \mathbb{Z}, p \nmid b \right\},$$

with maximal ideal $\mathfrak{m} = (p)$; this is the *localization* of the ring $\mathbb{Z}$ at the prime ideal (p). The residue field is $\mathbb{Z}_{(p)}/p\mathbb{Z}_{(p)} \simeq \mathbb{Z}/p\mathbb{Z} \simeq \mathbb{F}_p$.

Example 1.15. For any field k, the valuation $v\colon k((t)) \to \mathbb{Z} \cup \{\infty\}$ on the field of Laurent series over k defined by

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

where $a_{n_0} \neq 0$, has valuation ring $k[[t]]$, the power series ring over k. For $f \in k((t))^\times$, the valuation $v(f) \in \mathbb{Z}$ is the *order of vanishing* of f at zero. For every $\alpha \in k$ one can similarly define a valuation v_α on k as the order of vanishing of f at α by taking the Laurent series expansion of f about α.

1.5 Discrete Valuation Rings

Discrete valuation rings are in many respects the nicest rings that are not fields. In addition to being an integral domain, every discrete valuation ring A enjoys the following properties:

- *noetherian*: Every increasing sequence $I_1 \subseteq I_2 \subseteq \cdots$ of ideals eventually stabilizes; equivalently, every ideal is finitely generated.
- *principal ideal domain*: Every ideal is principal (generated by a single element).
- *local*: There is a unique maximal ideal $\mathfrak{m}$.
- *dimension one*: The (Krull) *dimension* of a ring R is the supremum of the lengths n of all chains of prime ideals $\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_n$ (which need not be finite, in general). For DVRs, $(0) \subseteq \mathfrak{m}$ is the longest chain of prime ideals, with length 1.
- *regular*: The dimension of the $A/\mathfrak{m}$-vector space $\mathfrak{m}/\mathfrak{m}^2$ is equal to the dimension of A. Non-local rings are regular if this holds for every localization at a prime ideal.
- *integrally closed* (or *normal*): Every element of the fraction field of A that is the root of a monic polynomial in $A[x]$ lies in A.
- *maximal*: There are no intermediate rings strictly between A and its fraction field.

Various combinations of these properties can be used to uniquely characterize discrete valuation rings (and hence give alternative definitions).

Theorem 1.16. *For an integral domain A, the following are equivalent:*

- *A is a DVR.*
- *A is a noetherian valuation ring that is not a field.*
- *A is a local PID that is not a field.*
- *A is an integrally closed noetherian local ring of dimension one.*
- *A is a regular noetherian local ring of dimension one.*
- *A is a noetherian local ring whose maximal ideal is nonzero and principal.*
- *A is a maximal noetherian ring of dimension one.*

Proof. See [1, §23] or [2, §9]. □

1.6 Integral extensions

Integrality plays a key role in number theory, so it is worth discussing it in more detail.

Definition 1.17. Given a ring extension $A \subseteq B$, an element $b \in B$ is *integral over A* if is a root of a monic polynomial in $A[x]$. The ring B is *integral over A* if all its elements are.

Proposition 1.18. *Let $\alpha, \beta \in B$ be integral over $A \subseteq B$. Then $\alpha + \beta$ and $\alpha\beta$ are integral over A.*

Proof. Let $f \in A[x]$ and $g \in A[y]$ be such that $f(a) = g(b) = 0$, where

$$f(x) = a_0 + a_1 x + \cdots + a_{m-1}x^{m-1} + x^m,$$
$$g(y) = b_0 + b_1 y + \cdots + b_{n-1}y^{n-1} + y^n.$$

It suffices to consider the case

$$A = \mathbb{Z}[a_0, \ldots, a_{m-1}, b_0, \ldots, b_{n-1}], \qquad \text{and} \qquad B = \frac{A[x,y]}{(f(x), g(y))},$$

with α and β equal to the images of x and y in B, respectively, since given any $A' \subseteq B'$ we have homomorphisms $A \to A'$ defined by $a_i \to a_i$ and $b_i \to b_i$ and $B \to B'$ defined by $x \mapsto \alpha$ and $y \mapsto \beta$, and if $x + y, xy \in B$ are integral over A then $\alpha + \beta, \alpha\beta \in B'$ must be integral over A'.

Let k be the algebraic closure of the fraction field of A, and let $\alpha_1, \ldots, \alpha_m$ be the roots of f in k and let $\beta_1, \ldots, \beta_n$ be the roots of g in k. The polynomial

$$h(z) = \prod_{i,j} \bigl(z - (\alpha_i + \beta_j)\bigr)$$

has coefficients that may be expressed as polynomials in the symmetric functions of the α_i and β_j, equivalently, the coefficients a_i and b_j of f and g, respectively. Thus $h \in A[z]$, and $h(x+y) = 0$, so $x+y$ is integral over A. Applying the same argument to $h(z) = \prod_{i,j}(z - \alpha_i\beta_j)$ shows that xy is also integral over A. □

Definition 1.19. Given a ring extension B/A, the ring $\tilde{A} = \{b \in B : b \text{ is integral over } A\}$ is the *integral closure of A in B*. When $\tilde{A} = A$ we say that A is *integrally closed in B*. For a domain A, its *integral closure* (or *normalization*) is its integral closure in its fraction field, and A is *integrally closed* (or *normal*) if it is integrally closed in its fraction field.

Proposition 1.20. *If $C/B/A$ is a tower of ring extensions in which B is integral over A and C is integral over B then C is integral over A.*

Proof. See [1, Thm. 10.27] or [2, Cor. 5.4]. □

Corollary 1.21. *If B/A is a ring extension, then the integral closure of A in B is integrally closed in B.*

Proposition 1.22. *The ring $\mathbb{Z}$ is integrally closed.*

Proof. We apply the rational root test: suppose $r/s \in \mathbb{Q}$ is integral over $\mathbb{Z}$, where r and s are coprime integers. Then

$$\left(\frac{r}{s}\right)^n + a_{n-1}\left(\frac{r}{s}\right)^{n-1} + \cdots a_1\left(\frac{r}{s}\right) + a_0 = 0$$

for some $a_0, \ldots, a_{n-1} \in \mathbb{Z}$. Clearing denominators yields

$$r^n + a_{n-1}sr^{n-1} + \cdots a_1 s^{n-1} r + a_0 s^n = 0,$$

thus $r^n = -s(a_{n-1}r^{n-1} + \cdots a_1 s^{n-2} r + a_0 s^{n-1})$ is a multiple of s. But r and s are coprime, so $s = \pm 1$ and therefore $r/s \in \mathbb{Z}$. □

Corollary 1.23. *Every unique factorization domain is integrally closed. In particular, every PID is integrally closed.*

Proof. The proof of Proposition 1.22 works for any UFD. □

Example 1.24. The ring $\mathbb{Z}[\sqrt{5}]$ is not a UFD (nor a PID) because it is not integrally closed: consider $\phi = (1+\sqrt{5})/2 \in \operatorname{Frac}\mathbb{Z}[\sqrt{5}]$, which is integral over $\mathbb{Z}$ (and hence over $\mathbb{Z}[\sqrt{5}]$), since $\phi^2 - \phi - 1 = 0$. But $\phi \notin \mathbb{Z}[\sqrt{5}]$, so $\mathbb{Z}[\sqrt{5}]$ is not integrally closed.

The corollary implies that every discrete valuation ring is integrally closed. In fact, more is true.

Proposition 1.25. *Every valuation ring is integrally closed.*

Proof. Let A be a valuation ring with fraction field k and let $\alpha \in k$ be integral over A. Then

$$\alpha^n + a_{n-1}\alpha^{n-1} + a_{n-2}\alpha^{n-2} + \cdots + a_1\alpha + a_0 = 0$$

for some $a_0, a_1, \ldots, a_{n-1} \in A$. Suppose $\alpha \notin A$. Then $\alpha^{-1} \in A$, since A is a valuation ring. Multiplying the equation above by $\alpha^{-(n-1)} \in A$ and moving all but the first term on the LHS to the RHS yields

$$\alpha = -a_{n-1} - a_{n-1}\alpha^{-1} - \cdots - a_1\alpha^{2-n} - a_0\alpha^{1-n} \in A,$$

contradicting our assumption that $\alpha \notin A$. It follows that A is integrally closed. □

Definition 1.26. A *number field* K is a finite extension of $\mathbb{Q}$. The *ring of integers* $\mathcal{O}_K$ is the integral closure of $\mathbb{Z}$ in K.

Remark 1.27. The notation $\mathbb{Z}_K$ is also sometimes used to denote the ring of integers of K. The symbol $\mathcal{O}$ emphasizes the fact that $\mathcal{O}_K$ is an *order* in K; in any $\mathbb{Q}$-algebra K of finite dimension r, an order is a subring of K that is also a free $\mathbb{Z}$-module of rank r, equivalently, a $\mathbb{Z}$-lattice in K that is also a ring. In fact, $\mathcal{O}_K$ is the *maximal order* of K: it contains every order in K.

Proposition 1.28. *Let A be an integrally closed domain with fraction field K. Let α be an element of a finite extension L/K, and let $f \in K[x]$ be its minimal polynomial over K. Then α is integral over A if and only if $f \in A[x]$.*

Proof. The reverse implication is immediate: if $f \in A[x]$ then certainly α is integral over A. For the forward implication, suppose α is integral over A and let $g \in A[x]$ be a monic polynomial for which $g(\alpha) = 0$. In $\overline{K}[x]$ we may factor $f(x)$ as

$$f(x) = \prod_i (x - \alpha_i).$$

For each α_i we have a field embedding $K(\alpha) \to \overline{K}$ that sends α to α_i and fixes K. As elements of $\overline{K}$ we have $g(\alpha_i) = 0$ (since $f(\alpha_i) = 0$ and f must divide g), so each $\alpha_i \in \overline{K}$ is integral over A and lies in the integral closure $\tilde{A}$ of A in $\overline{K}$. Each coefficient of $f \in K[x]$ can be expressed as a sum of products of the α_i, and is therefore an element of the ring $\tilde{A}$ that also lies in K. But $A = \tilde{A} \cap K$, since A is integrally closed in its fraction field K. □

Example 1.29. We saw in Example 1.24 that $(1+\sqrt{5})/2$ is integral over $\mathbb{Z}$. Now consider $\alpha = (1+\sqrt{7})/2$. Its minimal polynomial $x^2 - x - 3/2 \notin \mathbb{Z}[x]$, so α is not integral over $\mathbb{Z}$.

References

[1] Allen Altman and Steven Kleiman, *A term of commutative algebra*, Worldwide Center of Mathematics, 2013.

[2] Michael Atiyah and Ian MacDonald, *Introduction to commutative algebra*, Addison–Wesley, 1969.

[3] Pierre Deligne, *La conjecture de Weil: I*, Publications Mathématiques l'I.H.É.S. **43** (1974), 273–307.

[4] Jean-Pierre Serre, *Local fields*, Springer, 1979.

[5] André Weil, *Numbers of solutions of equations in finite fields*, Bulletin of the American Mathematical Society, **55** (1949), 497–508.

18.785 Number Theory I
Fall 2019