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 arithmetic, every element of $\mathbb{Z}$ can be written uniquely as a product of primes (up to 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 ($\mathbb{Z}$ is a ring of dimension one), and the residue field $\mathbb{Z}/p\mathbb{Z}$ is the finite field $\mathbb{F}_p$ with p elements (which is unique up to isomorphism). The fraction field of $\mathbb{Z}$ is the field $\mathbb{Q}$ of rational numbers, and together $\mathbb{Q}$ and the finite fields $\mathbb{F}_p$ of prime order make up the prime fields; every field k contains exactly one of them, according to its characteristic: zero if k contains $\mathbb{Q}$, and p if k contains $\mathbb{F}_p$.

The structure of the ring $\mathbb{Z}$ and the distribution of its prime elements is intimately related to the Reimann zeta function

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

This is a function of the complex variable s that is holomorphic and nonvanishing for $\mathrm{Re}(s) > 1$, and as we shall see it has 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 location 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), and as you are probably aware it is conjectured that they all lie on the *critical line* $\mathrm{Re}(s) = \frac{1}{2}$, this is the Riemann Hypothesis; 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 ideal; 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 first part 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, is a finite field $\mathbb{F}_{q^d}$, 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; for the field of rational numbers $\mathbb{Q}$, these 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 $\mathbb{F}_q[t]$. These rings have dimension one, which means that every nonzero prime ideal is maximal; thus each nonzero prime ideal has an associated *residue field*, and for both $\mathbb{Z}$ and $\mathbb{F}_q[t]$ these residue fields are finite. In the

case of $\mathbb{Z}$ we have residue fields $\mathbb{Z}/p\mathbb{Z} \simeq \mathbb{F}_p$ for each prime p, and for $\mathbb{F}_q[t]$ we have residue fields $\mathbb{F}_{q^d}$ associated to each irreducible polynomial of degree d.

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 in finite extensions of their fraction fields, known as *rings of integers*, and the prime ideals in these rings of integers. Where possible we will treat number fields and function fields on an equal footing, but we will also note some key differences. Perhaps somewhat surprisingly, the function field setting often turns out to be simpler than the number field setting, and considering the analogies between the two can provide insight into both.

While the topics above are typically classified under the heading of algebraic number theory, a key tool for understanding global fields are their associated *zeta functions*, which have a more analytic flavor (at least in the number field setting). The most famous of these is the Riemann zeta function

$$\zeta(s) := \sum_{n\geq 1} n^{-s} = \prod_p (1-p^{-s})^{-1},$$

which can be viewed both as a sum over integers and a product over primes (an *Euler product*). As you are no doubt aware, the Riemann hypothesis is concerned with the location of the complex zeros of the function $\zeta(s)$ and is one of the major open problems in number theory. It is worth noting that 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 consider are 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. $|x+y| \le |x| + |y|$.

If in addition the stronger condition

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

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

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

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

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*. We say that v is a *discrete valuation* if the 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). The set

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

is the *valuation ring* of k (with respect to v). The unit group of A is

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

since $v(1/x) = v(1) - v(x) = -v(x)$ implies x is invertible if and only if $v(x) = 0$.

It is easy to verify that the valuation ring A is a (commutative) ring, and even an integral domain (if x and y are nonzero then $v(xy) = v(x) + v(y) \neq \infty$, so $xy \neq 0$), and k is its fraction field. Any integral domain A which is the valuation ring of its fraction field with respect to some discrete valuation is called a *discrete valuation ring* (DVR).

Let us now assume that A is a discrete valuation ring. Any element $\pi \in A$ for which $v(\pi) = 1$ is called a *uniformizer*. Such a uniformizer necessarily exists, since v maps A surjectively onto $\mathbb{Z}_{\geq 0}$. 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. Thus A is a unique factorization domain (UFD), and in fact a principal ideal domain (PID). Indeed, every nonzero ideal of A is equal to

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

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. It follows that the ideals of A are totally ordered (with the same order type as $\mathbb{Z}_{\geq 0}$), and the ideal

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

is the unique maximal ideal and only nonzero prime ideal of A. Rings with a unique maximal ideal are called *local rings*.

Definition 1.11. The *residue field* of a discrete valuation ring A with unique 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 $\mathfrak{m} = (\pi)$, for any nonzero $x \in A$ we must have $v(x) = n$, where n is the least integer for which $x \in (\pi^n)$ (note that $(\pi^0) = (1) = A$, so such an n exists and is nonnegative); the integer n does not depend on the choice of the uniformizer π. Defining $v(0) = \infty$ and extending v to the fraction field 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.

Example 1.12. For the p-adic valuation $v_p\colon \mathbb{Q} \to \mathbb{Z} \cup \{\infty\}$ we have the valuation ring

$$\mathbb{Z}_{(p)} := \left\{ \frac{a}{b} : a, b \in \mathbb{Z}, p \not| b \right\},$$

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 1.13. 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 (a DVR cannot be a field because its maximal ideal $\mathfrak{m} = (\pi)$ is not the zero ideal: $v(\pi) = 1 \neq \infty$). 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 in A eventually stabilizes; equivalently, every ideal is finitely generated.
- *principal ideal domain*: not only is every ideal finitely generated, every ideal can be generated by a single element.
- *local*: A has a unique maximal ideal $\mathfrak{m}$.
- *dimension one*: the *height* of a prime ideal $\mathfrak{p}$ is the supremum of the lengths n 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). If A is a DVR then $\dim A = 1$, since $(0) \subseteq \mathfrak{m}$ is the longest chain of prime ideals in A.
- *regular*: The dimension of the $A/\mathfrak{m}$-vector space $\mathfrak{m}/\mathfrak{m}^2$ is the dimension of A. When A is not already local, this applies to its localizations at prime ideals.
- *integrally closed* (or *normal*): A contains every element of its fraction field that is integral over A (the root of a monic polynomial in $A[x]$).
- *maximal*: There are no intermediate rings strictly between A and its fraction field.

There are several different combinations of these properties that uniquely characterize discrete valuation rings (and hence may be taken as alternative definitions).

Theorem 1.14. *For an integral domain A, the following are equivalent:*

1. *A is a DVR.*
2. *A is a PID with a unique nonzero prime ideal.*
3. *A is an integrally closed noetherian local ring of dimension one.*

4. *A is a regular noetherian local ring of dimension one.*
5. *A is a noetherian local ring whose maximal ideal is nonzero and principal.*
6. *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 1.15. 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 1.16. *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

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

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 $a_i \to \mathfrak{a}_i$ 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 in A then $\alpha + \beta, \alpha\beta \in B'$ must be integral in A'.

Let k be the algebraic closure of the fraction field of B, 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

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

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 1.17. 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 1.18. *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 1.19. *If B/A is a ring extension, then the integral closure of A in B is integrally closed in B.*

Proposition 1.20. *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 1.21. *Every unique factorization domain is integrally closed.*

Proof. The proof of Proposition 1.20 works for any UFD. □

Example 1.22. The ring $\mathbb{Z}[\sqrt{5}]$ is not a UFD 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.

Definition 1.23. 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 1.24. 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 1.25. *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 $g(\alpha_i) = 0$, so each $\alpha_i \in \overline{K}$ is integral over A and lies in the integral closure $\bar{A}$ 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 $\bar{A}$ that also lies in K. But $A = \bar{A} \cap K$, since A is integrally closed in its fraction field K. □

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* **55** (1949), 497–508.

18.785 Number Theory I
Fall 2016