An Introduction to Abstract Algebra[1]

Andrew Klapper[2] and Mark Goresky[3]

[2]Department of Computer Science, 307 Marksbury Building, University of Kentucky, Lexington, KY, 40506. www.cs.uky.edu/∼klapper

[3]School of Mathematics, Inst. for Advanced Study, Princeton, NJ,08540. www.math.ias.edu/∼goresky

This document is an introduction to a variety of topics in modern algebra. It is extracted from a book on algebraically defined pseudorandom sequences and the set of topics is geared to that purpose. There is an emphasis, for example, on finite fields and adic rings. The beginning sections, however, are quite general and can serve as an introduction to the algebra needed for such topics as coding theory and cryptography. There is a bibliography that contains many general books on algebra.

Table of Contents

Chapter 1 Abstract Algebra

Abstract algebra plays a fundamental role in many areas of science and engineering. In this chapter we describe a variety of basic algebraic structures that play roles in the generation and analysis of sequences, especially sequences intended for use in communications and cryptography. This include groups (see Section 1.1), rings (see Section 1.2), and polynomials over rings (see Section 1.4). We also explore characters and Fourier transforms, basic tools for understanding structures based on groups and rings (see Section 1.3).

1.1 Group theory

Groups are among the most basic building blocks of modern algebra. They arise in a vast range of applications, including coding theory, cryptography, physics, chemistry, and biology. They are commonly used to model symmetry in structures or sets of transformations. They are also building blocks for more complex algebraic constructions such as rings, fields, vector spaces, and lattices.

1.1.a Basic properties

Definition 1.1.1. *A* group *is a set G with a distinguished element e (called the* identity*) and a binary operation $*$ satisfying the following axioms:*

1. *(Associative law) For all $a, b, c \in G$, $(a * b) * c = a * (b * c)$.*
2. *(Identity law) For all $a \in G$, $a * e = e * a = a$.*
3. *(Inverse law) For all $a \in G$, there exists $b \in G$ such that $a * b = e$. The element b is called an* inverse *of a.*

A group G is commutative *or* Abelian *if it also satisfies the following axiom:*

4. *(Commutative law) For all $a, b \in G$, $a * b = b * a$.*

The *order* of a group G, denoted $|G|$, is its cardinality as a set.

Proposition 1.1.2. *Let G be a group. Then the following statements hold.*

1. *If $a, b \in G$ and $a * b = e$ then $b * a = e$.*
2. *Every $a \in G$ has a unique inverse.*
3. *The identity $e \in G$ is unique.*

Proof. To prove the first claim, suppose $a*b = e$. Let c be an inverse of b. By associativity we have $(b*a)*b = b*(a*b) = b*e = b$. Therefore $e = b*c = ((b*a)*b)*c = (b*a)*(b*c) = (b*a)*e = b*a$.

To prove the second claim, suppose $a * b = e = a * c$. Then $b = e * b = (b * a) * b = b * (a * b) = b * (a * c) = (b * a) * c = e * c = c$.

To prove the third claim, suppose e and f are both identities in G. Then $e * f = e$ since e is an identity, and $e * f = f$ since f is an identity. Thus $e = f$. □

Sometimes we use *multiplicative notation* and write a^{-1} to denote the inverse of a, ab for $a * b$, $a^0 = e$, and $a^n = aa^{n-1}$ for n a positive integer. Then $a^n a^m = a^{n+m}$ and $(a^n)^m = a^{nm}$. If G is Abelian, it is common to use *additive notation* in which we write $+$ instead of $*$, $-a$ instead of a^{-1}, $a - b$ for $a + (-b)$, and 0 instead of e. Also, $0a = 0$ and $na = a + (n-1)a$ for n a positive integer. Then $na + ma = (n + m)a$ and $n(ma) = (nm)a$. We sometimes write $e = e_G$ when considering several different groups.

Examples:

1. The integers $\mathbb{Z}$ with identity 0 and addition as operation is an Abelian group.

2. The rational numbers $\mathbf{Q}$ with identity 0 and addition as operation is an Abelian group.

3. The nonzero rational numbers $\mathbf{Q} - \{\mathbf{0}\}$ with identity 1 and multiplication as operation is an Abelian group.

4. If S is any set, the set of permutations of S is a (non-Abelian if $|S| \geq 3$) group with composition as operation and the identity function as identity. The order of the permutation group of S is $|S|!$.

5. For any $n \geq 1$, the set of invertible $n \times n$ matrices (that is, with nonzero determinant) with rational entries is a (non-Abelian if $n \geq 2$) group with multiplication as operation and the $n \times n$ identity matrix as identity.

6. If $N \geq 2$, a, and b are integers, then a is congruent to b modulo N, written $a \equiv b \pmod{N}$, if N divides $a - b$. This is an equivalence relation on $\mathbb{Z}$. Let $\mathbb{Z}/(N)$ denote the set of equivalence classes for this relation. That is, $\mathbb{Z}/(N)$ is the set of sets of the form

$$a + N\mathbb{Z} = \{a + Nb : b \in \mathbb{Z}\}.$$

Then $\mathbb{Z}/(N)$ is an Abelian group with the operation $(a + N\mathbb{Z}) + (b + N\mathbb{Z}) = (a + b) + N\mathbb{Z}$ and $0 + \mathbb{Z}$ as identity. To prove this it suffices to show that this definition of addition is independent of the choice of representatives a and b (that is, if $a + N\mathbb{Z} = c + N\mathbb{Z}$ and $b + N\mathbb{Z} = d + m\mathbb{Z}$, then $(a + b) + N\mathbb{Z} = (c + d) + N\mathbb{Z}$) and that the group axioms for $\mathbb{Z}/(N)$ follow immediately from the

group axioms for $\mathbb{Z}$. We have $|\mathbb{Z}/(N)| = N$. The elements of $\mathbb{Z}/(N)$ are sometimes referred to as *residues* mod N.

The set of equivalence classes of elements that are relatively prime to m, denoted $(\mathbb{Z}/(N))^\times$, is also an Abelian group, with multiplication as operation and 1 as unit. We denote the order of this group by $\phi(N)$, Euler's totient function (or "ϕ" function). That is, $\phi(N)$ is the number of positive integers less or equal to than m and relatively prime to m. We also define $\phi(1) = 1$. We say more about Euler's totient function in Section 1.2.d.

Following is a basic fact about groups that we use later.

Theorem 1.1.3. *If G is a finite group and $a \in G$, then $a^{|G|} = e$.*

Proof. First suppose that G is Abelian. Let us define a function from G to itself by $f(b) = ab$. This function is one-to-one (if $ab = ac$ then multiplying by a^{-1} on the left gives $b = c$), so it is also a permutation of G. Therefore

$$\prod_{b\in G} b = \prod_{b\in G} ab = a^{|G|} \prod_{b\in G} b.$$

Multiplying by the inverse of

$$\prod_{b\in G} b$$

gives the result of the theorem.

Now suppose that G is arbitrary. Nonetheless,

$$H = \{a^i : i = 0, 1, \cdots\}$$

is an Abelian group, so $a^{|H|} = e$. Thus it suffices to show that $|H|$ divides $|G|$. Consider the cosets bH with $b \in G$. Suppose two of these have a nonempty intersection, $bH \cap cH \neq \emptyset$. Then there are integers i, j so that $ba^i = ca^j$. It follows from this that every ba^k is in cH and every ca^k is in bH. That is, $bH = cH$. This implies that the set of all cosets bH forms a partition of G. Since each bH has cardinality $|H|$, $|G|$ is a multiple of $|H|$ as desired. □

1.1.b Subgroups

In this section we examine subsets of group that inherit a group structure of their own.

Definition 1.1.4. *If G is a group, then a subset $H \subseteq G$ is a subgroup if it is a group with the same operation as G and the same identity as G.*

This means that H is a subset of G such that (1) $e \in H$; (2) if $a, b \in H$, then $a + b \in H$; and (3) if $a \in H$, then $a^{-1} \in H$. Then the group axioms hold in H. Also, if G is Abelian then H is Abelian.

For example, the additive group of integers is a subgroup of the additive group of rational numbers. The set of cyclic permutations of $\{1, 2, \cdots, n\}$ is a subgroup of the group of all permutations.

If G_1 and G_2 are groups with operations $*_1$ and $*_2$ and identities e_1 and e_2, then their *direct product* $G_1 \times G_2 = \{(a, b) : a \in G_1, b \in G_2\}$ is a group with operation $(a, b) * (c, d) = (a * c, b * d)$ and identity (e_1, e_2). More generally, if $\{G_i : i \in I\}$ is any collection of groups, indexed by a set I, then the Cartesian product

$$\prod_{i \in I} nG_i$$

is a group, again called the direct product of $\{G_i : i \in I\}$. The group operation is defined coordinate-wise. If all the groups are Abelian, then so is the product. If $I = \{1, 2, \cdots, n\}$ for some natural number n, then we write

$$\prod_{i \in I} nG_i = \prod_{i=1}^{n} G_i = G_1 \times G_2 \times \cdots \times G_n.$$

If $a \in G$ then we let $\langle a \rangle$ denote $\{a^i : i \in \mathbb{Z}\}$. This set is an Abelian subgroup, called the *subgroup generated by* a. If $|\langle a \rangle| < \infty$ then we say the *order of* a is this cardinality, $|\langle a \rangle|$. Otherwise we say a has infinite order. Equivalently, the order of a is the least $k > 0$ such that $a^k = e$, if such a k exists. A group is *cyclic* if $G = \langle a \rangle$ for some a and then a is called a generator of G. Every cyclic group is Abelian. The group $\mathbb{Z}/(N)$ is cyclic with generator 1. It is sometime referred to as the *cyclic group of order* N.

We need a basic lemma from number theory.

Lemma 1.1.5. *Let a, b be integers. Then there exist integers s, t with $\gcd(x, y) = sx + ty$.*

Proof. First we may assume that x and y are nonnegative since we can negate x or y without changing either $\gcd(x, y)$ or the set of integers of the form $sx + ty$. We can also assume $y \leq x$.

Now we proceed by induction on y. If $y = 0$, then $\gcd(x, y) = x$ and we can take $s = 1$ and $t = 0$. Otherwise, let $x = ay + z$ with $0 \leq z < y$. Then by induction there exist integers u, v with $\gcd(y, z) = uy + vz$. But $\gcd(x, y) = \gcd(y, z) = uy + v(x - ay) = vx + (u - av)y$ as claimed. □

Theorem 1.1.6. *Every subgroup of a cyclic group is cyclic. Suppose $\langle a \rangle$ is a finite cyclic group with order n.*

1. *If k is a positive integer, then $\langle a^k \rangle$ is a subgroup of $\langle a \rangle$ of order $n/\gcd(n, k)$.*
2. *If $d|n$ and $d > 0$, then $\langle a \rangle$ contains one subgroup of order d.*

3. If $d|n$ and $d > 0$, then $\langle a \rangle$ contains $\phi(d)$ elements of order d.
4. $\langle a \rangle$ contains $\phi(n)$ generators.

Proof. Let H be a nontrivial subgroup of $\langle a \rangle$. H contains some a^k with $k > 0$. Let k be the smallest positive integer with $a^k \in H$ and let $a^m \in H$. Suppose k does not divide m. Then $\gcd(k, m) < k$ and $\gcd(k, m) = sk + tm$ for some integers s, t. Indeed, every common divisor ofThen

$$a^{\gcd(k,m)} = (a^k)^s (a^m)^t \in H,$$

which is a contradiction. Therefore $H = \langle a^k \rangle$. Thus every subgroup of $\langle a \rangle$ is cyclic.

(1) Let $H = \langle a^k \rangle$ and $b = \gcd(n, k)$. We have $(a^k)^r = e$ if and only if $n|kr$. Thus the order of H is the least positive r such that $n|kr$. This is equivalent to $(n/b)|(k/b)r$, and this is equivalent to $(n/b)|r$. That is, the order of H is n/b.

(2) By (1), a subgroup $H = \langle a^k \rangle$ has order $d|n$ if and only if $d = n/\gcd(n, k)$, or, equivalently, $d \cdot \gcd(n, k) = n$. Let $b = \gcd(n, k) = sn + tk$ for some $s, t \in \mathbb{Z}$. Then $e = a^n \in H$, so $a^b \in H$ as above. Since $b|k$, we also have $H = \langle a^b \rangle$. But $b = n/d$ so H is the unique subgroup of order d. Conversely, $\langle a^{n/d} \rangle$ is a subgroup of order d, proving existence.

(3) Let $n = df$. By (1), an element a^k has order d if and only if $\gcd(n, k) = n/d = f$. This holds precisely when $k = gf$ with g relatively prime to $n/f = d$ and $0 < k < n$. That is, $0 < g < d$. The number of such g is $\phi(d)$.

(4) Follows immediately from (3) with $d = n$. □

For example, the group $\mathbb{Z}$ is cyclic (with generator 1) so every subgroup is of the form $m\mathbb{Z} = \{mk : k \in \mathbb{Z}\}$ for some integer m.

1.1.c Homomorphisms

More generally, relationships between groups often arise as functions from one group to another that preserve all the relevant algebraic structures and operations.

Definition 1.1.7. *Let G and H be two groups. A function $\varphi : G \to H$ is a* homomorphism *if it preserves the group operations. That is, if for every $a, b \in G$ we have $\varphi(ab) = \varphi(a)\varphi(b)$. The* image *of φ, denoted by* $\mathrm{Im}(\varphi)$*, is the set of $b \in H$ such that there is $a \in G$ with $\varphi(a) = b$. The* kernel *of φ, denoted by* $\mathrm{Ker}(\varphi)$*, is the set of $a \in G$ such that $\varphi(a) = e_H$. The homomorphism φ is an* endomorphism *if $G = H$. It is an* epimorphism *or is* surjective *if it is onto as a set function. It is a* monomorphism *or is* injective *if it is one-to-one as a set function. It is an* isomorphism *if it is both injective and surjective. It is an* automorphism *if it is an endomorphism and an isomorphism.*

If G is a group and $a \in G$, then we can define the function $\varphi(n) = a^n$. This function is a homomorphism and is a monomorphism if and only if a has infinite order. If a has finite order

m, then φ induces a monomorphism from $\mathbb{Z}/m\mathbb{Z}$ to G. In particular, every infinite cyclic group is isomorphic to the integers $\mathbb{Z}$ and every finite cyclic group is isomorphic to the (additive) group $\mathbb{Z}/(m)$ where m is the order of any generator.

Proposition 1.1.8. *Let $\varphi : G \to H$ be a homomorphism. Then φ preserves identity elements and inverses. Morever* $\mathrm{Ker}(\varphi)$ *is a subgroup of G and* $\mathrm{Im}(\varphi)$ *is a subgroup of H.*

Proof. To see that φ preserves identities observe that $\varphi(e_G) = \varphi(e_G e_G) = \varphi(e_G)\varphi(e_G)$. Multiplying by $\varphi(e_G)^{-1}$ then gives $e_H = \varphi(e_G)$. To see that φ preserves inverses, let $a \in G$. Then $e_H = \varphi(e_G) = \varphi(aa^{-1}) = \varphi(a)\varphi(a^{-1})$ so $\varphi(a)^{-1} = \varphi(a^{-1})$ by uniqueness of inverses. The remaining statements are left to the reader. □

Proposition 1.1.9. *If $\varphi : F \to G$ and $\psi : G \to H$ are homomorphisms, then the composition $\psi \circ \varphi : F \to H$ is a homomorphism.*

Proof. For all $a, b \in F$, we have $(\psi \circ \varphi)(a + b) = \psi(\varphi(ab)) = \psi(\varphi(a)\varphi(b)) = \psi(\varphi(a))g(\varphi(b))$. □

Definition 1.1.10. *A pair of homomorphisms $\varphi : F \to G$ and $\psi : G \to H$ is* exact *(at G) if the kernel of ψ equals the image of φ. A sequence of maps*

$$1 \to F \to G \to H \to 1 \tag{1.1}$$

is a short exact sequence *if it is exact at F, G, and H. Here 1 denotes the trivial group with a single element.*

The short exact sequence in (1.1) splits *if there is a homomorphism $\mu : H \to G$ so that $g \cdot h$ is the identity.*

Note that in equation (1.1), exactness at F is equivalent to φ being injective and exactness at H is equivalent to ψ being surjective.

Proposition 1.1.11. *If $1 \to F \to G \to H \to 1$ is a short exact sequence and all three groups are finite, then $|G| = |F| \cdot |H|$.*

Proof. Let φ denote the homomorphism from F to G, and let ψ denote the homomorphism from G to H. Since ψ is surjective, there is a subset U of G that maps one to one and onto H. If b is any element of G, then there is some $u \in U$ so that $\psi(u) = \psi(b)$. Then bu^{-1} maps to the identity in H, so $bu^{-1} = a \in \mathrm{Im}(\varphi)$. Thus we can write $b = au$ with $a \in \mathrm{Im}(\varphi)$. Suppose that $au = a'u'$ for some $a, a' \in \mathrm{Im}(\varphi)$ and $u, u' \in U$. Then $u'u^{-1} = (a')^{-1}a \in \mathrm{Im}(\varphi)$. It follows that $\psi(u'u^{-1}) = e_H$, so $\psi(u') = \psi(u)$. By the choice of U, we have $u = u'$. Then also $a = a'$. It follows that for each b there is a unique representation in the form $b = au$. The proposition is follows from this. □

Proposition 1.1.12. *Suppose* $1 \to F \to G \to H \to 1$ *is a short exact sequence with* $\varphi : F \to G$ *and* $\psi : G \to H$*, all three groups are Abelian, and the short exact sequence splits via a homomorphism* $h : H \to G$*, then there is an isomorphism between* $F \times H$ *and* G *given by* $(a, b) \mapsto \varphi(a)\mu(b)$*. Conversely, if* $G = F \times H$*, then there is a short exact sequence as in (1.1), where* ψ *is the projection map and* φ *maps* a *to* $(a, 1)$*.*

Proof. In Proposition 1.1.11 we can take U to be the image of μ to prove the first statement. The converse is trivial. □

1.1.d Quotients

If m is any positive integer, then the set of multiples of m, $m\mathbb{Z}$, is a subgroup of the (additive) group $\mathbb{Z}$. In Sect. 1.1.a the *quotient group* $\mathbb{Z}/m\mathbb{Z}$ is defined as the set of equivalence classes of $\mathbb{Z}$ under the following equivalence relation: $a \equiv b \pmod{m}$ if $a - b \in m\mathbb{Z}$.

More generally, suppose G is any group and H is a subgroup of G. Define an equivalence relation by saying $a \sim b$ if there is an $h \in H$ such that $b = ah$ (The proof that this is an equivalence relation is left as an exercise). The equivalence class of a is $aH = \{ah : \ h \in H\}$ and is called the *left coset of* a. The set of left cosets is denoted G/H. It is not always possible to form a group out of these cosets (but see Sect. 1.1.e).

In fact, we could have started by defining $a \sim' b$ if there is an $h \in H$ such that $b = ha$. This is also an equivalence relation. The equivalence class Ha of a with respect to this relation is called the *right coset of* a, the set of which is denoted $H\backslash G$. If G is Abelian, then $Ha = aH$ for all $a \in G$. More generally:

Definition 1.1.13. *If* H *is a subgroup of* G*, then* H *is* normal in G *if for every* $a \in G$*, we have* $aH = Ha$ *or equivalently, if* $aha^{-1} \in H$ *for every* $a \in G$ *and every* $h \in H$*.*

Theorem 1.1.14. *If* H *is normal in* G*, then* $G/H = H\backslash G$ *is a group under the operation* $(aH)(bH) = abH$*.* □

In this case, G/H is called the *quotient group of* G *modulo* H. The natural mapping $G \to G/H$ (given by $a \mapsto aH$) is a homomorphism. If the set of left cosets is finite, then we say H has *finite index* in G. The number of left cosets (which equals the number of right cosets) is called the *index of* H *in* G. Thus if H is normal in G and of finite index, then G/H is finite and $|G/H|$ equals the index of H in G. If G is finite, so is G/H, and we have $|G/H| = |G|/|H|$.

Theorem 1.1.15. *If* $\varphi : G \to G'$ *is a homomorphism then the following statements hold.*

1. $\mathrm{Ker}(\varphi)$ *is normal in* G*.*
2. *The quotient* $G/\mathrm{Ker}(\varphi)$ *is isomorphic to* $\mathrm{Im}(\varphi)$*.*

3. *Conversely, if H is a normal subgroup of G, then the natural mapping $a \mapsto aH$ is a surjection from G to G/H with kernel equal to H.*

□

Thus if H is normal in G, then we have a short exact sequence

$$1 \to H \to G \to G/H \to 1.$$

1.1.e Conjugacy and groups acting on sets

Two elements a and b in a group G are *conjugate* if there is an element $g \in G$ such that $b = gag^{-1}$. This is an equivalence relation on G whose equivalence classes are called *conjugacy classes*. If G is Abelian, then every conjugacy class has a single element, but if $ab \neq ba$, then both a and bab^{-1} are distinct elements in the same conjugacy class. Thus the number of conjugacy classes gives some measure of how far G is from being Abelian. If H and H' are subgroups of G, we say they are conjugate if there is an element $g \in G$ such that $H' = hHg^{-1}$.

An *action* of a group G on a set S is a mapping $G \times S \to S$, written $(g, s) \mapsto g \cdot s$, such that $(gh) \cdot s = g \cdot (h \cdot s)$ for all $g, h \in G$ and all $s \in S$. It follows that the identity $e \in G$ acts trivially ($e \cdot s = s$) and that each $g \in G$ acts by permutations. The *orbit* of an element $s \in S$ is the set

$$G \cdot s = \{g \cdot s : \ g \in G\}.$$

If $H \subset G$ is a subgroup then G acts on G/H by $g \cdot xH = (gx) \cdot H$.

If G acts on S, and if $s \in S$, define the *stabilizer* or *isotropy subgroup*,

$$\mathrm{Stab}_G(s) = \{g \in G : \ g \cdot s = s\}.$$

It is a subgroup of G. If $s, s' \in S$ are in a single orbit then their stabilizers are conjugate. In fact if $s' = gs$ then $\mathrm{Stab}_G(s') = g\mathrm{Stab}_G(s)g^{-1}$. The action of G on S is *transitive* if there is a single orbit, i.e., for every $s, s' \in S$ there exists $g \in G$ such that $s' = g \cdot s$. Suppose this to be the case, choose a "base point" $s_0 \in S$, and let $H = \mathrm{Stab}_G(s_0)$. This choice determines a one to one correspondence $\varphi : G/H \to S$ with $\varphi(gH) = g \cdot s_0$. The mapping φ is then compatible with the actions of G on G/H and on S, that is, $g \cdot \varphi(xH) = \varphi(g \cdot xH)$ for all $g \in G$ and all $xH \in G/H$. If $|G| < \infty$ it follows that $|S| = |G|/|H|$ divides $|G|$.

The group G acts on itself by translation ($g \cdot x = gx$) and by conjugation ($g \cdot x = gxg^{-1}$). The first action is transitive; the second is not, and its orbits are the conjugacy classes of G.

1.1.f Finitely generated Abelian groups

An Abelian group G is *finitely generated* if there is a finite set $V \subseteq G$ such that every element of G is equal to a finite product of elements of V. We state without proof the fundamental theorem of finite Abelian groups (See, for example, Lang [20, p. 46]):

Theorem 1.1.16. *Let G be a finitely generated Abelian group. Then G is isomorphic to a direct product of cyclic groups.*

Corollary 1.1.17. *Let G be a finite Abelian group with nm elements, where n and m are relatively prime positive integers. Then there are groups H_1 and H_2 with n and m elements, respectively, so that G is isomorphic to $H_1 \times H_2$.*

An element g in an Abelian group G is a *torsion* element if $g \neq 0$ and if some finite sum $g + g + \cdots + g = 0$ vanishes. That is, if it has finite order. The group G is *torsion-free* if it contains no torsion elements.

Corollary 1.1.18. *Let G be a finitely generated torsion-free Abelian group. Then G is isomorphic to a direct product of finitely many copies of $\mathbb{Z}$.*

1.2 Rings

Many important algebraic structures come with two interrelated operations. For example, addition and multiplication of integers, rational numbers, real numbers, and complex numbers; AND and XOR of Boolean valued functions; and addition and multiplication of $n \times n$ matrices of integers, etc.

Definition 1.2.1. *A ring R is a set with two binary operations $+$ and $\cdot$ and two distinguished elements $0, 1$ which satisfy the following properties for all $a, b, c \in R$:*

1. *R is an Abelian group with operation $+$ and identity 0;*
2. *$a \cdot (b \cdot c) = (a \cdot b) \cdot c$ and $1 \cdot a = a \cdot 1 = a$; and*
3. *$a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ and $(b + c) \cdot a = (b \cdot a) + (c \cdot a)$ (the distributive law).*

It follows that $a \cdot 0 = 0$ for all a, since $a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 + a \cdot 0$. If $0 = 1$ then $R = \{0\}$ is the zero ring. It is common to denote by R^+ the Abelian group that is obtained from R by forgetting the multiplication operation.

A ring R is *commutative* if $a \cdot b = b \cdot a$ for all $a, b \in R$. *Throughout this book, all rings are commutative unless otherwise stated.* We generally write ab for the product $a \cdot b$.

1.2.a Units and zero divisors

Let R be a commutative ring. An element $a \in R$ is a *unit* if it is invertible, that is, if there exists $b \in R$ so that $ab = 1$. In this case b is unique. The collection of all units in R is denoted $R^\times$. It forms an Abelian group (under multiplication). An element $a \in R$ is a *zero divisor* if there exists a nonzero element $b \in R$ such that $ab = 0$. The ring of integers $\mathbb{Z}$ has no zero divisors, but only

1 and -1 are units. However if the ring R is finite then a given element is either a unit or a zero divisor. Indeed, let $\varphi_a : R \to R$ be the mapping which is given by multiplication by a. If φ_a is one to one, then it is also onto, hence a is invertible. If φ_a is not one to one, then there exist $b \neq c$ so that $ab = ac$ or $a(b-c) = 0$, so a is a zero divisor. If $a, b \in R$ and $ab = 0$, then b is said to *annihilate* a, and the set of such b is called the *annihilator* of a, denoted Z_a.

Let $b \in R$ be a unit. The smallest integer $m > 0$ such that $b^m = 1$ is called the multiplicative *order* of b, if such an $m < \infty$ exists; otherwise b is said to have infinite order. If $b \in R$ has order $m < \infty$, if $u \in R$ and if $t > 0$ is the smallest integer such that $(b^t - 1)u = 0$ then t divides m. (For, the group $\mathbb{Z}/(m)$ acts transitively on the set $\{u, bu, \cdots, b^{t-1}u\}$ with $k \in \mathbb{Z}/(m)$ acting by multiplication by b^k.) In particular, if $s > 0$ is relatively prime to m then $b^s - 1$ is not a zero divisor in R

Definition 1.2.2. *An* integral domain *(also called an* entire ring*) is a commutative ring with no zero divisors. A field is a commutative ring in which every nonzero element is invertible.*

In particular, a finite integral domain is necessarily a field. Every commutative ring R embeds in a ring $S^{-1}R$ which has the property that every element is either a zero divisor or is invertible, cf. Section 1.2.e.

1.2.b Ideals and quotients

Definition 1.2.3. *A* subring *S of a ring R is a subset of R, which is a ring under the same operations as R, and with the same zero and identity.*

If I is an additive subgroup of R (meaning that if $a, b \in I$ then $a + b \in I$ and $-a \in I$) then the quotient R/I is the set of equivalence classes under the equivalence relation $a \sim b$ if $a - b \in I$. The equivalence class containing $a \in R$ is the coset $a + I$. Then R/I is an Abelian group under addition: $(a + I) + (b + I) = a + b + I$. However, the multiplication operation on R does not necessarily induce a well defined multiplication on R/I. For if $a' \sim a$, say, $a' = a + c$ and if $b' \sim b$, say, $b' = b + d$ (where $c, d \in I$) then $a'b' = ab + ad + bc + cd$ which is not equivalent to ab unless $ad + bc + cd \in I$. The following definition is necessary and sufficient to ensure this holds for all $a, b \in R$ and $c, d \in I$.

Definition 1.2.4. *An ideal is an additive subgroup $I \subset R$ such that for any $a \in I$ and for any $b \in R$ we have $ab \in I$.*

It follows that the set of equivalence classes R/I inherits a ring structure from R if and only if I is an ideal. Two elements $a, b \in R$ are said to be *congruent modulo I* if they are in the same equivalence class. That is, if $a - b \in I$. Each equivalence class is called a *residue class modulo I*.

An ideal I is *proper* if $I \neq R$, in which case it does not contain any units. An ideal I is *principal* if there exists an element $a \in R$ such that $I = \{ar : r \in R\}$, in which case we write

$I = (a)$. If I, J are ideals then the sum $I + J$ is the set of all sums $a + b$ where $a \in I$ and $b \in J$. It is an ideal and is the smallest ideal containing both I and J. The intersection $I \cap J$ is also an ideal. The *product ideal* IJ is the set of all finite sums $\sum a_i b_i$ where $a_i \in I$ and $b_i \in J$. An ideal $I \subset R$ is *maximal* if I is proper and is not a proper subset of any other proper ideal. An ideal I is *prime* if $ab \in I$ implies $a \in I$ or $b \in I$. An ideal $I \subset R$ is *primary* if $I \neq R$ and whenever $ab \in I$, either $a \in I$ or $b^n \in I$ for some $n \geq 1$.

A field contains only the ideals (0) and (1).

Theorem 1.2.5. *Let R be a commutative ring. Then the following statements hold.*

1. *An ideal $P \subset R$ is maximal if and only if R/P is a field (called the* residue field with respect to P*).*
2. *An ideal $P \subset R$ is prime if and only if R/P is an integral domain. (See Definition 1.2.13.)*
3. *Every maximal ideal is prime.*

Proof. (1) Let P be maximal and $a \in R - P$. Then $J = \{ab + c : b \in R, c \in P\}$ is closed under addition and under multiplication by elements of R. It contains P (take $b = 0$) and a (take $b = 1$ and $c = 0$) so it properly contains P. By maximality it is not a proper ideal, so it must not be a proper subset of R. That is, $J = R$. In particular, $1 \in J$, so $1 = ab + c$ for some $b \in R$ and $c \in P$. Therefore $(a+P)(b+P) = ab+P = 1-c+P = 1+P$ so $a+P$ is invertible in R/P. Thus R/P is a field. On the other hand, suppose R/P is a field and J is an ideal containing P. Let $a \in J - P$. Then $a + P$ is invertible in R/P, so there is a $b \in R$ such that $(a + P)(b + P) = 1 + P$. That is, such that $ab = 1 + c$ for some $c \in P$. But then $1 = ab - c \in J$. By closure under multiplication by R, we have $R \subseteq J$. But this contradicts the fact that J is an ideal. Therefore P is maximal.

(2) Let $a, b \in R$. Then $(a + P)(b + P) = 0$ in R/P if and only if $ab \in P$. If P is prime, this says $(a + P)(b + P) = 0$ implies $a \in P$ or $b \in P$, which implies $a + P = 0$ or $b + P = 0$ in R/P, so R/P is an integral domain. Conversely, if R/P is an integral domain, then $ab \in P$ implies $(a + P)(b + P) = 0$ which implies $a + P = 0$ or $b + P = 0$. That is, $a \in P$ or $b \in P$, so P is a prime ideal.

(3) This follows from (1) and (2). □

For example, consider the ring of ordinary integers $\mathbb{Z}$. Let I be an ideal containing a nonzero element. Multiplication by -1 preserves membership in I, so I contains a positive element. Let m be the least positive element of I. Suppose that $a \in I$ is any other element of I. Then $\gcd(m, a) = um + va$ for some integers u and v, so $\gcd(m, a) \in I$. We have $\gcd(m, a) \leq m$, so by the minimality of m, $\gcd(m, a) = m$. That is, m divides a. Since every multiple of m is in I, it follows that I consists exactly of the multiples of m. In particular, $I = (m)$ is principal.

The ideal (m) is contained in the ideal (n) if and only if m is a multiple of n. The ideal (m) is prime if and only if m is prime. In this case it is also maximal. It is primary if and only if m is a power of a prime.

Definition 1.2.6. *A function $\varphi : R \to S$ from a ring R to a ring S is a* ring homomorphism *if $\varphi(a+b) = \varphi(a)+\varphi(b)$ and $\varphi(ab) = \varphi(a)\varphi(b)$ for all $a, b \in R$. The homomorphism φ is a* surjection *(or* epimorphism*) if it is onto. It is an* injection *(or* monomorphism*) if it is one to one. It is an* isomorphism *if it is both an injection and a surjection. It is an* endomorphism *if $R = S$. It is an* automorphism *if it is an endomorphism and an isomorphism.*

The set of automorphisms of a ring S forms a group under composition, denoted by $\mathrm{Aut}(S)$. More generally, if R is a subring of S (we also say that S is an *extension of* R), then the set of automorphisms of S whose restrictions to R are the identity forms a subgroup $\mathrm{Aut}_R(S)$. The proof of the following theorem is left as an exercise.

Theorem 1.2.7. *If $\varphi : R \to S$ is a ring homomorphism, then*

$$\mathrm{Ker}(\varphi) = \{\mathrm{r} \in \mathrm{R} : \ \varphi(\mathrm{r}) = 0\}$$

is an ideal of R, the image of φ is a subring of S, and φ induces an isomorphism between $R/\mathrm{Ker}(\varphi)$ and $\mathrm{Im}(\varphi)$. Conversely, if I is an ideal of R then the map $a \mapsto a+I$ is a surjective homomorphism from $R \to R/I$ with kernel I.

If $f : R \to S$ is a surjective ring homomorphism with kernel $I \subset R$, then

$$0 \to I \to R \to S$$

is a short exact sequence of additive groups. Sometimes there is also an injection $g : S \to R$ such that $f \circ g$ is the identity function (a *right inverse* of f). In this case it makes sense to think of S as a subring of R so that R is an algebra over S. We say that g is a *splitting* of f.

If R is a ring and $a \in R$, then the annihilator Z_a of a is an ideal. It is proper because $1 \notin Z_a$.

1.2.c Characteristic

Let R be a commutative ring. If m is a nonnegative integer, we write $m \in R$ for the sum $1+1\cdots+1$ (m times). This defines a homomorphism from $\mathbb{Z}$ into R. That this function is a homomorphism can be shown by a series of induction arguments. In fact this is the unique homomorphism from $\mathbb{Z}$ into R, since any such homomorphism is completely determined by the facts that $1_{\mathbb{Z}}$ maps to 1_R, and the ring operations are preserved. The kernel of this homomorphism is an ideal in $\mathbb{Z}$, hence by the example in Section 1.2.b is of the form (m) for some nonnegative integer m. This integer is called the *characteristic* of R. For any $a \in R$, we have $ma = a+a+\cdots+a$ (m times). Hence if the characteristic is nonzero, it is the smallest positive integer m such that $ma = 0$ for all $a \in R$. If the characteristic is zero, then no such m exists and $\mathbb{Z}$ is isomorphic to a subring of R. Otherwise $\mathbb{Z}/(m)$ is isomorphic to a subring of R. If R is finite then its characteristic is positive since the sequence of elements $1, 2, 3, \cdots \in R$ must eventually lead to a repetition.

Theorem 1.2.8. *If R is an integral domain then its characteristic is either 0 or is a prime number. In particular, the characteristic of any finite field is prime.*

Proof. Suppose R is an integral domain. Let $k > 0$ be the characteristic and suppose $k = mn$ (in $\mathbb{Z}$), with $m, n > 0$. Then $mn = 0$ in R, so $m = 0$ or $n = 0$ in R. Suppose $m = 0$. For any $c \in R$, the element $c + \cdots + c$ (m times) is $mc = 0$. By the minimality of k, we must have $m = k$ and $n = 1$. A similar argument holds when $n = 0$ in R. It follows that k is prime. □

Lemma 1.2.9. *Let R be a commutative ring. If the characteristic k of R is a prime number, and if q is any positive power of k then*

$$(a + b)^q = a^q + b^q \in R \tag{1.2}$$

for every $a, b \in R$.

Proof. Suppose k is prime and $0 < m < k$. The binomial coefficient

$$\binom{k}{m} = \frac{k!}{m!(k-m)!}$$

is divisible by k since k appears as a factor in the numerator but not in the denominator. Consequently $(a + b)^k = a^k + b^k$ and equation (1.2) follows by induction. □

If k is not prime, then equation (1.2) is generally false.

1.2.d The Ring $\mathbb{Z}/(N)$ and primitive roots

In this section we continue the example of the modular integers introduced in Section 1.1.a. Fix a nonzero integer N. The ring $\mathbb{Z}/(N)$ is the (cyclic) group of order N, $\mathbb{Z}/(N)$, together with the operation of multiplication. The same symbol is used for both structures, which often causes some confusion. The group $\mathbb{Z}/(N)$ is sometimes referred to as the *additive group* of $\mathbb{Z}/(N)$. The characteristic of the ring $\mathbb{Z}/(N)$ is $|N|$.

As in Section 1.2.c, the mapping $\pmod N : \mathbb{Z} \to \mathbb{Z}/(N)$ is a ring homomorphism. If $x \in \mathbb{Z}$ we sometimes write $\overline{x} \in \mathbb{Z}/(N)$ for its reduction modulo N. Conversely, it is customary to represent each element $y \in \mathbb{Z}/(N)$ by the corresponding integer $\widehat{y} \in \mathbb{Z}$ with $0 \le \widehat{x} \le N - 1$, but note that this association $\mathbb{Z}/(N) \to \mathbb{Z}$ is neither a group nor a ring homomorphism. It is also common to omit the "bar" and the "hat", thereby confusing the integers between 0 and $N - 1$ with $\mathbb{Z}/(N)$.

If m divides N then the mapping $\pmod m : \mathbb{Z}/(N) \to \mathbb{Z}/(m)$ is a ring homomorphism. If a, b are nonzero, relatively prime integers, then the mapping

$$\mathbb{Z}/(ab) \to \mathbb{Z}/(a) \times \mathbb{Z}/(b) \tag{1.3}$$

given by $x \mapsto (x \pmod a, x \pmod b)$ is a ring isomorphism. (Since both sides have the same number of elements it suffices to check that the kernel is zero. But if x is divisible by a and by b and if a, b are relatively prime, then x is divisible by ab. This is a special case of the *Chinese remainder theorem*, Theorem 1.2.18).

Let $x \in \mathbb{Z}$. The following statements are equivalent:

1. The element $\overline{x} = x \pmod N \in \mathbb{Z}/(N)$ is invertible in $\mathbb{Z}/(N)$.

2. The element $\overline{N} = N \pmod x \in \mathbb{Z}/(x)$ is invertible in $\mathbb{Z}/(x.)$

3. The integers x and N are relatively prime.

4. There exists $n > 0$ so that $x|(N^n - 1)$

5. There exists $m > 0$ so that $N|(x^m - 1)$

6. The element $\overline{x} \in \mathbb{Z}/(N)$ generates the *additive* group of $\mathbb{Z}/(N)$. That is, the elements $\{0, \overline{x}, \overline{x} + \overline{x}, \overline{x} + \overline{x} + \overline{x}, \cdots\}$ account for all the elements in $\mathbb{Z}/(N)$.

As we saw in Section 1.2.c, the units in $\mathbb{Z}/(N)$ form an Abelian group under multiplication, the *multiplicative group* $\mathbb{Z}/(N)^\times$. Euler's totient function, $\phi(N) = |\mathbb{Z}/(N)^\times|$ is defined to be the number of units in $\mathbb{Z}/(N)$. For any $y \in \mathbb{Z}/(N)^\times$ there is a least power d, called the *order* of y and denoted $d = \mathrm{ord}_N(y)$, such that $y^d = 1 \in \mathbb{Z}/(N)$. It follows from Theorem 1.1.3 that $d|\phi(N)$, so if y is relatively prime to N then $y^{\phi(N)} \equiv 1 \pmod N$, which is called *Fermat's congruence* or Fermat's little theorem. The least n, m in (4), (5) is $n = \mathrm{ord}_x(\overline{N})$ and $m = \mathrm{ord}_N(\overline{x})$ respectively.

Lemma 1.2.10. *Let N be a positive integer. Then the following statements hold.*

1. *If $N = \prod_{i=1}^k p_i^{m_i}$ is the prime factorization of N then $\phi(N) = \prod_{i=1}^k \phi(p_i^{m_i})$.*

2. *$\phi(p^m) = p^{m-1}(p-1)$ if p is prime.*

3. *$N = \sum_{d|N} \phi(d)$.*

Proof. The first statement follows from equation (1.3). In the second statement, since p is prime, the only integers that are not relatively prime to p^m are the multiples of p. There are p^{m-1} of these in $\mathbb{Z}/(p^m)$, which leaves $p^{m-1}(p-1)$ integers that are relatively prime to p, proving the second statement. (In fact, the group $\mathbb{Z}/(p^m)^\times$ is described in Section 3.2.a: it is cyclic of order $p^{n-1}(p-1)$ if $p > 2$. If $p = 2$ and $m \geq 3$ then it is a product of two cyclic groups, one of order 2

(generated by -1) and one of order p^{m-1}, generated by 5.) For the third statement, consider the set of fractions $\{1/N, 2/N, \cdots, N/N\}$. They are distinct, positive, and ≤ 1. Reduce each of these to its lowest terms. Then the denominator of each fraction will be a divisor d of N. For a given denominator d the possible numerators will be any integer relatively prime to d and $\leq d$, so there are $\phi(d)$ of them. Therefore, adding $\phi(d)$ over all $d|N$ gives N. □

From the comments in the preceding paragraph, it follows that the multiplicative group $\mathbb{Z}/(N)^\times$ is cyclic if and only if $N = p^m, 2p^m, 2$, or 4, where $p \geq 3$ is an odd prime. In this case a generator $a \in \mathbb{Z}/(N)^\times$ is called a *primitive root* modulo N. The number of primitive roots modulo N is therefore $\phi(\phi(N))$. The *Artin conjecture* states in part that each prime number $p \in \mathbb{Z}$ is a primitive root modulo q for infinitely many primes q. The following proposition helps enormously in verifying primitivity modulo a prime power p^t.

Lemma 1.2.11. *Let p be prime and let $s \geq 1, t \geq 1, b \in \mathbb{Z}$. Then b is a unit modulo p^s if and only if it is a unit modulo p^t.*

Proof. We may assume that $s = 1$. If a is a unit modulo p^t, then $p^t|bc - 1$ for some b, so $p|bc - 1$ as well, and b is a unit modulo p.

Conversely, suppose b is a unit modulo p, so $p|bc - 1$ for some c. We claim by induction that for all i there is a c_i so that $p^i|bc_i - 1$. Indeed, for $i \geq 2$ by induction let

$$bc_{i-1} = 1 + p^{i-1}d_{i-1}.$$

Then by the binomial theorem,

$$(bc_{i-1})^p = (1 + p^{i-1}d_{i-1})^p = 1 + p^i d_{i-1} + (p^{i-1})^2 z$$

for some integer z. But $2(i-1) = 2i - 2 \geq i$, so

$$b(b^{p-1}c_{i-1}^p) \equiv 1 \pmod{p^i}$$

as claimed. In particular, b is a unit modulo p^t. □

Proposition 1.2.12. *Suppose $N = p^t$ with $p \geq 3$ an odd prime and $t \geq 2$. Let $2 \leq a \leq N - 1$. Then a is primitive modulo N if and only if a is primitive modulo p^2. This holds if and only if a is primitive modulo p, and p^2 does not divide $a^{p-1} - 1$.*

Proof. If a is primitive modulo p^t, then by Lemma 1.2.11 every unit b modulo p or p^2 is a unit modulo p^t. Thus b is congruent to a power of a modulo t, and hence also modulo p and p^2. Thus a it is primitive modulo p and p^2. We prove the converse by induction on t, following [13, Section 4.1 Theorem 2]. Fix $t \geq 3$ and suppose that a is primitive in $\mathbb{Z}/(p^s)$ for all $s < t$. The order of

a is a divisor of $\phi(p^t) = p^{t-1}(p-1)$, the cardinality of the group of units in $\mathbb{Z}/(p^t)$. We want to show that the order of a is not a divisor of $p^{t-1}(p-1)/r$, for any prime divisor r of $p^{t-1}(p-1)$. First we take $r = p$. Since

$$a^{p^{t-3}(p-1)} = a^{\phi(p^{t-2})} \equiv 1 \pmod{p^{t-2}}$$

we have

$$a^{p^{t-3}(p-1)} = 1 + cp^{t-2}$$

for some $c \neq 0$, and c is relatively prime to p since a is primitive for $\mathbb{Z}/(p^{t-1})$. Then

$$a^{p^{t-2}(p-1)} = (1 + cp^{t-2})^p \equiv 1 + cp^{t-1} \not\equiv 1 \pmod{p^t}$$

since $\binom{p}{i}$ is a multiple of p. This shows that the order of a modulo p^t is not $\phi(p^t)/r$ with $r = p$.

Now suppose that r is a prime divisor of $p-1$ and

$$a^{p^{t-1}(p-1)/r} \equiv 1 \pmod{p^t}.$$

Let b be a primitive element modulo p^t and $a \equiv b^k \pmod{p^t}$. Then

$$b^{kp^{t-1}(p-1)/r} \equiv 1 \pmod{p^t}$$

so $p^{t-1}(p-1)$ divides $kp^{t-1}(p-1)/r$. Equivalently, r divides k. But then

$$a^{p^{t-2}(p-1)/r} \equiv b^{kp^{t-2}(p-1)/r} \equiv 1 \pmod{p^{t-1}}$$

as well and this is a contradiction. This proves the first statement.

We have shown that if a is primitive modulo p^t then a is primitive modulo p, and p^2 does not divide $a^{p-1} - 1$. Now we prove the converse. If p^2 does not divide $a^{p-1} - 1$, then the only way that a can fail to be primitive modulo p^2 is if a has order modulo p^2 dividing $p(p-1)/r$ for some prime divisor of $p-1$. But as we saw in the previous paragraph, this implies that a has order modulo p dividing $(p-1)/r$, which would contradict a's primitivity modulo p. □

1.2.e Divisibility in rings

Let R be a commutative ring. If $a, b \in R$ then a is a *divisor* of b if there exists $c \in R$ such that $ac = b$, in which case we write $a|b$. The element a is a *unit* if it is invertible, or equivalently, if it is a divisor of 1. Elements $a, b \in R$ are *associates* if $a = \epsilon b$ for some unit ϵ. A nonzero element $c \in R$ is a *common divisor* of a and b if $c|a$ and $c|b$. It is a *greatest common divisor* of a and b (written $c = \gcd(a, b)$) if it is a common divisor and if every other common divisor of a and b divides c. An element $c \neq 0$ is a *common multiple* of a and b if $a|c$ and $b|c$. It is a *least common multiple*

(written $c = \operatorname{lcm}(a, b)$) if it is a common multiple and if it divides every other common multiple of a and b.

A nonzero element $r \in R$ is *prime* if (r) is a proper prime ideal, meaning that if $ab \in (r)$ then $a \in (r)$ or $b \in (r)$. It is *primary* if (r) is primary, meaning that $ab \in (r)$ implies $a \in (r)$ or $b^n \in (r)$ for some $n > 0$. It is *irreducible* if it is not a unit and if $r = ab$ implies that a or b is a unit. Two nonzero non-units $r, s \in R$ are *coprime* or *relatively prime* if $(r) + (s) = R$ or equivalently if there exist $a, b \in R$ so that $1 = ar + bs$. See also Theorem 1.2.15.

Definition 1.2.13. *Let R be a commutative ring.*

1. *R is an* integral domain *(or simply a* domain*, or* entire*) if it has no zero divisors.*
2. *R is* principal *if every ideal in R is principal. It is a* principal ideal domain *or* PID *if it is principal and is an integral domain.*
3. *R is a* GCD ring *if every pair of elements has a greatest common divisor.*
4. *R is a* local ring *if it contains a unique maximal ideal (which therefore consists of the set of all non-units).*
5. *R is a* unique factorization domain *(or* UFD*, or* factorial*) if it is an integral domain and every nonunit $a \in R$ has a factorization into a product*

$$a = \prod_{i=1}^{m} p_i \tag{1.4}$$

   of irreducible elements (not necessarily distinct), which is unique up to reordering of the p_is and multiplication of the p_is by units. That is, if $a = \prod_{i=1}^{n} q_i$, then $m = n$ and there is a permutation σ of $\{1, \cdots, m\}$ so that p_i and $q_{\sigma(i)}$ are associates.
6. *R is a* factorization ring *if every nonunit $a \in R$ has a factorization into a product of irreducible elements, not necessarily distinct, and not necessarily in a unique way. An entire factorization ring is a* factorization domain*.*
7. *R is* Noetherian *if every increasing sequence of ideals $I_1 \subset I_2 \subset \cdots$ stabilizes at some finite point, or equivalently, if every ideal is finitely generated.*
8. *R is* Euclidean *if there is a function $\delta : R \to \{0, 1, 2, \cdots\} \cup \{-\infty\}$ such that (1) for every $a, b \in R$ with a and b both nonzero, we have $\delta(ab) \geq \delta(a)$, and (2) for every $a, b \in R$ with $b \neq 0$ there exist $q \in R$ (the quotient) and $r \in R$ (the remainder)*
   so that

$$a = qb + r \quad \text{and} \quad \delta(r) < \delta(b). \tag{1.5}$$

Theorem 1.2.14 summarizes the various inclusions among the special types of rings that we have discussed. We have included the polynomial ring $R[x]$ for ease of reference although it will not be considered until Section 1.4.

Theorem 1.2.14. *Let R be a commutative ring and let $R[x]$ be the ring of polynomials with coefficients in R (see Section 1.4). Then we have the following diagram of implications between various possible properties of R.*

$$\begin{array}{ccccccccccc} field & \Longrightarrow & Euclidean & \Longrightarrow & PID & \Longrightarrow & UFD & \Longrightarrow & entire & \Longrightarrow & R[x]entire \\ \Downarrow & & & & & & \Downarrow & & & & \\ R[x]Euclidean & & & & & & GCD & & & & \end{array}$$

If R is finite and entire then it is a field. If R is an order in an algebraic number field (see Section 2.4.c) then it is entire and Noetherian. The following additional implications hold.

$$\begin{array}{ccccccc} PID & \Longrightarrow & Noetherian & \Longrightarrow & factorization & & \\ & & \Downarrow & & & & factorization \\ & & R[x]Noetherian & \Longrightarrow & R[x]factorization & \Longleftarrow & domain + GCD \end{array}$$

Proof. The properties of the polynomial ring $R[x]$ are proved in Lemma 1.4.1 and Theorem 1.4.2. If R is a field then it is Euclidean with $\delta(0) = -\infty$ and $\delta(r) = 0$ for all nonzero elements $r \in R$.

To show that every Euclidean ring is a PID, let R be Euclidean. Suppose $a \in R$ is nonzero. We can write $0 = qa + r$ with $\delta(r) < \delta(a)$. Suppose that q is nonzero. Then $\delta(r) = \delta(-qa) \geq \delta(a)$, which is a contradiction. Thus $q = 0$ so $r = 0$. But then we must have $\delta(0) < \delta(a)$ for every $a \neq 0$. In particular, $\delta(a) \geq 0$ if a is nonzero. Now let I be a nonzero ideal in R. Let $a \in I - \{0\}$ be an element such that $\delta(a)$ is minimal. There is at least one such element since $\delta(I - \{0\}) \subset \mathbb{N}$ has a least element (by the well ordering principal). We claim that $I = (a)$. Let b be any other element in I. Then $b = qa + r$ for some $q, r \in R$ such that $\delta(r) < \delta(a)$. But $r = b - qa \in I$, so $r = 0$. That is, $b = qa$, as claimed. Moreover, if $0 = ab$ for some nonzero a, then the argument above shows that $b = 0$, so R is an integral domain.

Now assume that R is a PID. If a and b are two elements of R, then the ideal (a, b) has a principal generator, $(a, b) = (c)$. Thus c divides both a and b, and $c = ua + vb$ for some $u, v \in R$. Therefore any common divisor of a and b divides c as well. That is, c is a GCD of a and b. It follows that R is a GCD ring. It also follows that the GCD c can be written in the form $c = ua+vb$.

To see that R is Noetherian, let $I_1 \subset I_2 \subset \cdots$ be an increasing chain of ideals in R. The union of the I_ns is an ideal, so it is principal,

$$\cup_{n=1}^{\infty} I_n = (a)$$

for some a. But there is a natural number n with $a \in I_n$, so the chain stabilizes at I_n.

Suppose that R is Noetherian. We prove that R is a factorization ring. That is, that every element $a \in R$ has a prime factorization. Let S be the set of nonzero elements of R that do not have prime factorizations, and suppose S is nonempty. Let $a \in S$. Then a is not prime, so we

can write $a = bc$ with neither b nor c in (a). Since a is in S, either b or c is in S. Repeating this infinitely gives a chain $(a_1) \subset (a_2) \subset \cdots$ with $a_i \in S$ and $(a_i) \neq (a_{i+1})$ for every $i \geq 1$. This contradicts the fact that R is Noetherian.

Now we return to the case when R is a PID (and hence a GCD ring and Noetherian and so a factorization ring) and prove uniqueness of factorizations. Suppose $a \in R$ is irreducible and $a|bc$. If $a \not| b$, then 1 is a gcd of a and b, so we have

$$1 = ua + vb,$$

for some $u, v \in R$. Thus $c = uac + vbc$, so $a|c$. That is, if $a|bc$, then $a|b$ or $a|c$. In other words, a is prime if a is irreducible. Suppose some nonunit $b \in R$ can be factored in two ways,

$$b = \prod_{i=1}^{k} p_i = \prod_{i=1}^{\ell} q_i.$$

Since b is not a unit, we have $k > 0$ and $\ell > 0$. We use induction on k. Since $p_k | \prod_{i=1}^{\ell} q_i$, we have $p_k | q_n$ for some n by the primality of p_k, say $q_n = dp_1$. By the irreducibility of p_k and q_n, d is a unit. Then $\prod_{i=1}^{k-1} p_i = d(\prod_{i=1}^{\ell} q_i)/q_n$, and the result follows by induction. This completes the proof that a PID R is a UFD.

The implication UFD $\implies$ GCD is straightforward. Every UFD is an integral domain by definition. This completes the first diagram of implications.

The implication (finite + entire $\implies$ field) was proven in Section 1.2.a. An order R in a number field is a free $\mathbb{Z}$ module of finite rank, so the same is true of any ideal in R, hence such an ideal is finitely generated (as an Abelian group). Thus R is Noetherian.

The proof that (Noetherian $\implies$ $R[x]$ Noetherian) is fairly long and will be omitted; it is called Hilbert's basis theorem, see any book on commutative algebra, for example [1]. The remaining results involving polynomials are proved in Section 1.4.a. □

Theorem 1.2.15. *Let R be a commutative ring and let $a, b \in R$. Then*

1. *The element a is prime if and only if it has the following property: if $a|cd$ then $a|c$ or $a|d$.*
2. *If a is prime and is not a zero divisor, then a is irreducible.*
3. *If R is a UFD, then a is prime if and only if a is irreducible.*
4. *The elements a and b are coprime if and only if (the image of) a is invertible in $R/(b)$ (if and only if the image of b is invertible in $R/(a)$).*
5. *If a and b are coprime, then every common divisor of a and b is a unit.*
6. *If R is a PID and if every common divisor of a and b is a unit, then a and b are coprime.*
7. *If R is a PID and $a \in R$, then a is prime if and only if (a) is maximal (if and only if $R/(a)$ is a field).*

Proof. Part (1) is just a restatement of the definition that (a) is a prime ideal.

Now suppose a is prime and is not a zero divisor, and suppose $a = cd$. Then either $c \in (a)$ or $d \in (a)$; we may assume the former holds. Then $c = ea$ for some $e \in R$, so $a = cd = ead$ or $a(1 - ed) = 0$. Since a is not a zero divisor, we have $ed = 1$ hence d is a unit. This proves (2).

For part (3), first suppose that $a \in R$ is irreducible and let $cd \in (a)$. Then $cd = ae$ for some element $e \in R$. The right side of this equation is part of the unique factorization of the left side, so a must divide either c or d. Therefore either $c \in (a)$ or $d \in (a)$. The converse was already proven in part (2). (Note that a UFD contains no zero divisors, due to the unique factorization of 0.)

For part (4), if a is invertible in $R/(b)$ then there exists $c \in R$ so that $ac \equiv 1 \pmod{b}$, meaning that there exists $d \in R$ so that $ac = 1 + db$. Hence $(a) + (b) = R$. The converse is similar.

For part (5), supposing a and b are coprime, we may write $1 = ac + bd$ for some $c, d \in R$. If $e|a$ and $e|b$ then $a = fe$ and $b = ge$ for some $f, g \in R$. This gives $1 = (fc + gd)e$ so e is invertible.

For part (6), Suppose R is a PID. Given a, b the ideal $(a) + (b)$ is principal, so it equals (c) for some $c \in R$, which implies that $c|a$ and $c|b$. Therefore c is a unit, so $(a) + (b) = (c) = R$.

For part (7), we have already shown, in Theorem 1.2.5 that (a) maximal implies that a is prime. For the converse, suppose that (a) is prime and that $(a) \subset (b) \neq R$. Then b is not a unit, and $a = cb$ for some $c \in R$. Since the ring R is also a UFD, the element a is irreducible, so c is a unit. Therefore $(a) = (b)$ hence (a) must be maximal. □

1.2.f Examples

Here are a few standard examples of rings.

1. The integers $\mathbb{Z}$ is a Euclidean ring with $\delta(a) = |a|$.

2. The rational numbers $\mathbb{Q}$, the real numbers $\mathbb{R}$, and the complex numbers $\mathbb{C}$ are fields.

3. If $k = mn$ is a composite integer (with $m, n \geq 2$) then $\mathbb{Z}/k\mathbb{Z}$ is not an integral domain since $m \cdot n = 0$.

4. If R is a ring and S is a nonempty set, then the set of functions from S to R is a ring with the operations $(f + g)(x) = f(x) + g(x)$ and $(fg)(x) = f(x)g(x)$. The zero is the function $z(x) = 0$ for all x, and the identity is the function $i(x) = 1$ for all x.

5. If R is a ring then the collection $R[x]$ of polynomials with coefficients in R (see Section 1.4) is a ring.

6. Let G be an Abelian group with operation $*$ and identity e. The set E of endomorphisms of G is a ring with the operations $+_E$ = "product" and $\cdot_E$ = "composition". The zero is the function $z(a) = e$ for all a, and the identity is the function $i(a) = a$ for all a.

1.2.g The Euclidean algorithm

If R is Euclidean (and hence a GCD domain) via function $\delta : R \to \{0, 1, 2, \cdots\} \cup \{-\infty\}$, then the Euclidean algorithm, given in Figure 1.1, computes the gcd of any two elements. We assume that addition and multiplication of elements in R are atomic operations and that given $a, b \in R$, we can compute $q, r \in R$ as in equation (1.5). The algorithm assumes that a and b are nonnegative.

```
EUCLID(a, b)
    begin
    while (b ≠ 0) do
        Let a = qb + r
        (a, b) = (b, r)
     od
    return(a)
    end
```

Figure 1.1: The Euclidean Algorithm.

The proof of correctness of the Euclidean algorithm is essentially the same as in the integer case, which can be found in most general texts on algorithms. The time complexity depends on the ring, and in particular on the maximum time $M(d)$ it takes to compute q and r as in equation (1.5) when $\max(\delta(a), \delta(b)) \leq d$.

If $d = \max(\delta(a), \delta(b))$ decreases by an additive constant ϵ at each stage, then the complexity is at most $O(dM(d))$. This is the case when $R = \mathbb{F}[x]$ for a finite field F and $\delta(a) = \deg(a)$. In this case M is the time required to multiply polynomials, say $M(d) \in O(d \log(d))$ using fast Fourier transforms. The resulting complexity of the Euclidean algorithm is $O(\deg(a)^2 \log(\deg(a)))$. However a better bound can be found in this case by taking into account the degrees of the intermediate quotients. Two degree d polynomials can be divided in time $O(d(e + 1))$, where e is the degree of the quotient. Suppose that the sequence of polynomials produced by the algorithm is $r_0 = a, r_1 = b, r_2, \cdots, r_n$. Then $n \leq d$. If r_i has degree d_i, then the ith quotient has degree at most $d_{i-1} - d_i$. Thus the complexity is in

$$O(\sum_{i=0}^{d} d_{i-1}(d_{i-1} - d_i + 1)) \in O(d \sum_{i=1}^{d} (d_{i-1} - d_i + 1)) = O(d(d_0 - d_n + d)) = O(d^2).$$

If for some constant $\epsilon < 1$, $\delta(a)$ is decreased by a factor of ϵ after a constant number c of steps, then a simple bound on the complexity is $O(\log(d)M(d))$. This is the case when $R = \mathbb{Z}$

and $\delta(a) = |a|$. However a better bound can be found in this case by taking into account the actual numbers involved. Two k-bit numbers can be divided in time $O(k(\ell+1))$, where ℓ is the number of bits in the quotient. Suppose that the sequence of numbers produced by the algorithm is $r_0 = a, r_1 = b, r_2, \cdots, r_n$. Then $n \leq k$. If r_i has k_i bits, then the ith quotient has at most $k_{i-1} - k_i + 1$ bits. Thus the complexity is in

$$O(\sum_{i=1}^{k} k_{i-1}(k_{i-1} - k_i + 2)) \in O(k \sum_{i=1}^{k}(k_{i-1} - k_i + 2)) = O(k(k_0 - k_n + 2k)) = O(k^2) = O(\log(d)^2).$$

Theorem 1.2.16. *If $R = \mathbb{F}[x]$ for a finite field F, then the complexity of the Euclidean algorithm on inputs of degree $\leq d$ is in $O(d^2)$. If $R = \mathbb{Z}$, the the complexity of the Euclidean algorithm on inputs of size $\leq d$ is in $O(\log(d)^2)$.*

If R is a Euclidean domain, then (by Theorem 1.2.14) it is also a PID. If $a, b \in R$, then the ideal generated by a and b has a generator c. As in the proof of Theorem 1.2.14, $c = \gcd(a, b)$ and there are elements $u, v \in R$ so that $c = ua + vb$. The elements u and v are sometimes called *Bézout coefficients* It turns out that with a simple modification, the Euclidean algorithm can be used to compute the Bézout coefficients. This can be described by keeping track of all the intermediate information in the computation of the Euclidean algorithm:

$$r_0 = a, u_0 = 1, v_0 = 0;$$

$$r_1 = b, u_1 = 0, v_1 = 1;$$

and for $i \geq 1$

$$r_{i+1} = r_{i-1} - q_i r_i, u_{i+1} = u_{i-1} - q_i u_i, v_{i+1} = v_{i-1} - q_i v_i.$$

The sequence halts with $i = n$ so that $r_n = 0$. The sequence $(u_i, v_i, r_i), i = 0, 1, \cdots, n$ is called the *Bézout sequence of a and b*. We have the following facts on rational approximation of N-adic numbers using the Euclidean algorithm.

Lemma 1.2.17.

1. $r_1 > r_2 > \cdots > r_{n-1} = \gcd(a, b) \geq 0$.

2. *For $0 \leq i \leq n$,*
$$u_i a + v_i b = r_i. \tag{1.6}$$

3. *For $0 \leq i \leq n-1$,*
$$u_i v_{i+1} - u_{i+1} v_i = (-1)^i. \tag{1.7}$$

4. *If i is even then $u_i \geq 0$ and $v_i \geq 0$. If is odd then $u_i \geq 0$ and $v_i \geq 0$.*

5. *$|u_1| < |u_2| < \cdots |u_n|$ and $|v_0| < |v_1| < \cdots |v_n|$.*

6. *For $0 \leq i \leq n-1$, $|u_{i+1} r_i| \leq b$, $|v_{i+1} r_i| \leq a$, $|u_i r_{i+1}| \leq b$, and $|v_i r_{i+1}| \leq a$.*

1.2.h Fractions

The field of rational numbers $\mathbb{Q}$ is constructed from the ring of integers $\mathbb{Z}$ as the set of all fractions a/b, where we identify a/b with $(ax)/(bx)$ for any nonzero integer x. A similar construction can be made in great generality. Let R be a commutative ring. A subset S of R is *multiplicative* if it is closed under multiplication. If S is any multiplicative subset of R, define the ring $S^{-1}R$ to be the collection of all formal symbols a/b (where $a \in R$ and $b \in S$), under the following equivalence relation: $a/b \sim a'/b'$ if there exists $s \in S$ such that

$$s(ab' - ba') = 0. \tag{1.8}$$

Addition and multiplication of fractions are defined by the usual formulas:

$$\frac{a}{b} + \frac{a'}{b'} = \frac{ab' + a'b}{bb'} \quad \text{and} \quad \frac{a}{b}\frac{a'}{b'} = \frac{aa'}{bb'}.$$

The ring $S^{-1}R$ consists of a single element if $0 \in S$, so sometimes this case is excluded.

Now suppose that S does not contain any zero divisors (which will always be the case in our applications). Then equation (1.8) may be replaced by the more familiar equivalence relation: $ab' = a'b$. The natural mapping $R \to S^{-1}R$ (which takes a to $a/1$) is an injection, so $S^{-1}R$ "contains" R. Every element of S has become invertible in $S^{-1}R$. If the set S consists of all the elements that are not zero divisors, then an element of $S^{-1}R$ is either a zero divisor or else it is invertible. In this case, the ring $S^{-1}R$ is called the (full) *ring of fractions* of R. If R is an integral domain then its ring of fractions is a field, which is called the *fraction field* of R. See for example, Section 2.4.7, Section 4.2 and Section 4.4.

1.2.i Chinese remainder theorem

If R_1 and R_2 are rings then their Cartesian product $R_1 \times R_2$ is a ring under the coordinate-wise operations of addition and multiplication. The Chinese remainder theorem gives a sufficient condition under which a ring may be decomposed as a product.

Theorem 1.2.18. *Let R be a ring and let $I_1, \cdots, I_k$ be ideals such that $I_i + I_j = R$ for every $i \neq j$. Let*

$$I = \cap_{j=1}^{k} I_j.$$

Then for every $a_i, \cdots, a_k \in R$ there is an element $a \in R$ such that for every i, $a \equiv a_i \pmod{I_i}$. The element a is unique modulo I. Furthermore,

$$R/I \cong \prod_{j=0}^{k} R/I_j.$$

Proof. For $k = 1$ the statement is trivial. If $k = 2$, then there are elements $b_1 \in I_1$ and $b_2 \in I_2$ so that $1 = b_1 + b_2$. Let $a = a_1 b_2 + a_2 b_1$.

Now suppose $k > 2$. For every i let

$$J_i = \prod_{j \neq i} I_j.$$

For every $i \geq 2$ there are elements $c_i \in I_1$ and $b_i \in I_i$ such that $1 = c_i + b_i$. In particular,

$$\prod_{i=2}^{k} (c_i + b_i) = 1.$$

This product is in $I_1 + J_1$, so $R = I_1 + J_1$. Similarly, $R = I_j + J_j$ for every j. By the theorem in the case of two ideals, there is an element $d_j \in R$ such that $d_j \equiv 1 \pmod{I_j}$ and $d_j \equiv 0 \pmod{J_j}$. Then $a = a_1 d_1 + \cdots + a_k d_k$ satisfies our requirements

For each i there is a reduction homomorphism φ_i from R/I to R/I_i. This induces a homomorphism φ from R/I to

$$\prod_{j=1}^{k} R/I_j$$

whose kernel is

$$I = \bigcap_{j=1}^{k} I_j.$$

Thus φ is injective. By the first part it is surjective, hence an isomorphism. This also proves the uniqueness of a. □

Corollary 1.2.19. *Suppose R is a PID and $b_1, \cdots, b_k \in R$ are pairwise relatively prime. If $a_1, \cdots, a_k \in R$, then there exists an element $a \in R$ such that for every i, $a \equiv a_i \pmod{b_i}$.*

Proof. By Theorem 1.2.18 it suffices to show that for each $i \neq j$ we have $(b_i) + (b_j) = R$. The set $(b_i) + (b_j)$ is an ideal. Since R is a PID, there is some $b \in R$ so that $(b_i) + (b_j) = (b)$. This says that b is a common divisor of b_i and b_j, so b is a unit by assumption. Thus $(b_i) + (b_j) = R$. □

By Theorem 1.2.14, Corollary 1.2.19 applies in particular when R is a Euclidean domain. The case when $R = \mathbb{Z}$ is the classical Chinese Remainder Theorem.

1.2.j Vector spaces

In many settings we have a notion of one algebraic object "acting on" another by multiplication. For example, a real number r acts on the set of points in the plane by $(x, y) \mapsto (rx, ry)$.

Definition 1.2.20. *A* vector space *over a field F is a set V such that V is an Abelian group with an operation $+$, and there is a function $\cdot$ from $F \times V$ to V such that for all $a, b \in F$ and $u, v \in V$*

1. $a \cdot (u + v) = (a \cdot u) + (a \cdot v)$;
2. $(ab) \cdot u = a \cdot (b \cdot u)$;
3. $(a + b) \cdot u = (a \cdot u) + (b \cdot u)$; *and*
4. $1 \cdot u = u$.

It follows from these axioms that for every $u \in V$, $0 \cdot u = 0$.

For example, the set of points in the real plane is a vector space over the real numbers. If F is a field which is a subring of a ring R, then R is a vector space over F (just use the multiplication in R for the action of F on R). If F is a field and S is a nonempty set, then the set of functions from S to F is a vector space over F with the operations $(f+g)(x) = f(x)+g(x)$ and $(a \cdot f)(x) = af(x)$ for $a \in F$, $x \in S$, and $f, g : S \to F$. Various restrictions can be put on the functions to produce interesting vector spaces (e.g., continuity if $S = F = \mathbb{R}$).

Let V be a vector space over a field F. The elements of V are called *vectors*. A *linear combination* of vectors $v_1, v_2, \cdots, v_k \in V$ is a vector $a_1v_1 + a_2v_2 + \cdots + a_kv_k$ with $a_1, a_2, \cdots, a_k \in F$. A set of vectors $S \subseteq V$ is *linearly independent* if the only linear combination of elements of S that is zero is the one with all the coefficients a_i equal to zero. S *spans* V if every vector can be written as a linear combination of elements of S. S is a *basis* for V if it spans V and is linearly independent. The proof of the following is an exercise.

Theorem 1.2.21. *Let V be a vector space over a field F. If V has more than one element then it has a nonempty basis. If S is a basis, then every vector can be written uniquely as a linear combination of elements of S.*

If V has a basis S with a finite number of elements, then we say V is *finite dimensional with dimension* $= |S|$. In this case it can be shown that every basis has the same number of elements. In the important case when F is a subfield of a field E, E is called an *extension field*. If E is finite dimensional as a vector space over F, then its dimension is called *the degree of the extension* and is denoted $[E : F]$.

Theorem 1.2.22. *If F is a finite field and V is a finite dimensional vector space over F with dimension d, then $|V| = |F|^d$.*

Proof. Let S be a basis for V. Thus $|S| = d$. That is $S = \{v_1, v_2, \cdots, v_d\}$ for some $v_1, v_2, \cdots, v_d$. By the previous theorem, the elements of V are in one-to-one correspondence with the linear combinations $\sum_{i=1}^{d} a_i v_i$, $a_i \in F$. There are exactly $|F|^d$ such linear combinations. □

Definition 1.2.23. *If F is a field and V and W are vector spaces over F, then a function $L : V \to W$ is a* homomorphism *or is* F-linear *if it is a group homomorphism and for all $a \in F$ and $v \in V$ we have $L(av) = aL(v)$.*

If $S = \{v_1, v_2, \cdots, v_d\}$ is a basis for V, then an F-linear function L is completely determined by its values on the elements of S since

$$L\left(\sum_{i=1}^{d} a_i v_i\right) = \sum_{i=1}^{d} a_i L(v_i).$$

On the other hand, any choice of values for the $L(v_i)$ determines an F-linear function L. Furthermore, if $T = \{w_1, w_2, \cdots, w_e\}$ is a basis for W, then each value $L(v_i)$ can be expressed as a linear combination

$$L(v_i) = \sum_{j=1}^{e} b_{ij} w_j$$

with $b_{ij} \in F$.

Theorem 1.2.24. *If F is finite and V and W are finite dimensional with dimensions d and e, respectively, then there are $|F|^{de}$ F-linear functions from V to W.*

The image and kernel of L are Abelian groups, and it is straightforward to check that they are also vector spaces over F. Their dimensions are called the *rank* and *co-rank* of L, respectively. We leave it as an exercise to show that the rank plus the co-rank equals the dimension of V.

We can identify an element $\sum_i a_i v_i \in V$ with the column vector $(a_1, \cdots, a_d)^t$ (where the superscript t denotes the transpose of a matrix), and similarly for an element of W. Then the linear function L is identified with ordinary matrix multiplication by the matrix $B = [b_{ij}]$. The rank of L is the size of a maximal set of independent columns or independent rows of B.

If B is a square matrix, then the determinant of B is defined as usual in linear algebra. In this case the kernel is nonempty if and only if the determinant is zero.

If V and W are vector spaces over a field F, then the set of F-linear homomorphisms from V to W is denoted $\mathrm{Hom_F(V, W)}$. It is again a vector space over F with F acting by $(a \cdot L)(v) = L(av)$. By Theorem 1.2.24, if V and W are finite dimensional then the dimension of $\mathrm{Hom_F(V, W)}$ is the product of the dimensions of V and W.

In the special case when $W = F$, the dimension of $\mathrm{Hom_F(V, F)}$ is the same as that of V, so $\mathrm{Hom_F(V, F)}$ and are isomorphic as vector spaces over F (but not canonically – an isomorphism depends on a choice of bases). $\mathrm{Hom_F(V, F)}$ is called the *dual space* of V.

1.2.k Modules and lattices

The notion of a vector space over a field can be generalized to rings.

Definition 1.2.25. *Let $(R, +, \cdot, 0, 1)$ be a commutative ring. A* module over R *is an Abelian group $(M, +, 0_M)$ with an operation $\cdot$ from $R \times M$ to M such that for all $a, b \in R$ and $u, v \in M$*

1. $a \cdot (u + v) = (a \cdot u) + (a \cdot v)$;
2. $(ab) \cdot u = a \cdot (b \cdot u)$;
3. $(a + b) \cdot u = (a \cdot u) + (b \cdot u)$; *and*
4. $1 \cdot u = u$.

Again, it follows from these axioms that for every $u \in V$, $0 \cdot u = 0$.

For example, every Abelian group is a module over the integers (if $n \in \mathbb{Z}^+$, then $n \cdot a$ equals the sum of n copies of a). If f is a homomorphism from a ring R to a ring S, then S is a module over R with the operation $a \cdot u = f(a)u$.

It is apparent that the notion of basis does not make sense for modules in general – even a single element of a module may not be linearly independent. However, if there is a finite set of elements $m_1, \cdots, m_k \in M$ such that every element of M can be written (perhaps not uniquely) as a linear combination $a_1 m_1 + \cdots + a_k m_k$ with $a_1, \cdots, a_k \in R$, then we say that M is *finitely generated over* R. If M is finitely generated, then the size of the smallest set of generators for M over R is called the *R-rank* or simply the rank of M.

A module M over a ring R is *free* if M is isomorphic to the Cartesian product of a finite number of copies of R. That is, M is free if there are elements $m_1, \cdots, m_k \in M$ such that every element $m \in M$ can be represented uniquely in the form

$$m = \sum_{i=1}^{k} c_i m_i, \quad c_i \in R.$$

In this case the set $m_1, \cdots, m_k$ is called a basis of M over R.

Definition 1.2.26. *A* lattice L *is the set of integer linear combinations of a collection $U = \{u_1, \cdots, u_k\}$ of $\mathbb{R}$-linearly independent vectors in $\mathbb{R}^n$. The set U is called a* basis *for L. The lattice L is* full *if $k = n$, which we now assume. Then M_U is defined to be the matrix whose rows are $u_1, u_2, \cdots, u_n$. The volume of the parallelepiped spanned by these vectors is denoted $D_U = |\det(M_U)|$, and it is referred to as the* volume *of the lattice L, or the* determinant *of L.*

It is immediate that a lattice is a free $\mathbb{Z}$-module. A basis for a full lattice L is also a basis for $\mathbb{R}^n$. A full 2-dimensional lattice with basis $(5, 1)$, $(3, 4)$ is shown in Figure 1.2.k. The following theorem says that $\mathrm{vol}(L)$ is well-defined and it gives a way to tell when a collection of vectors forms a basis of a given lattice.

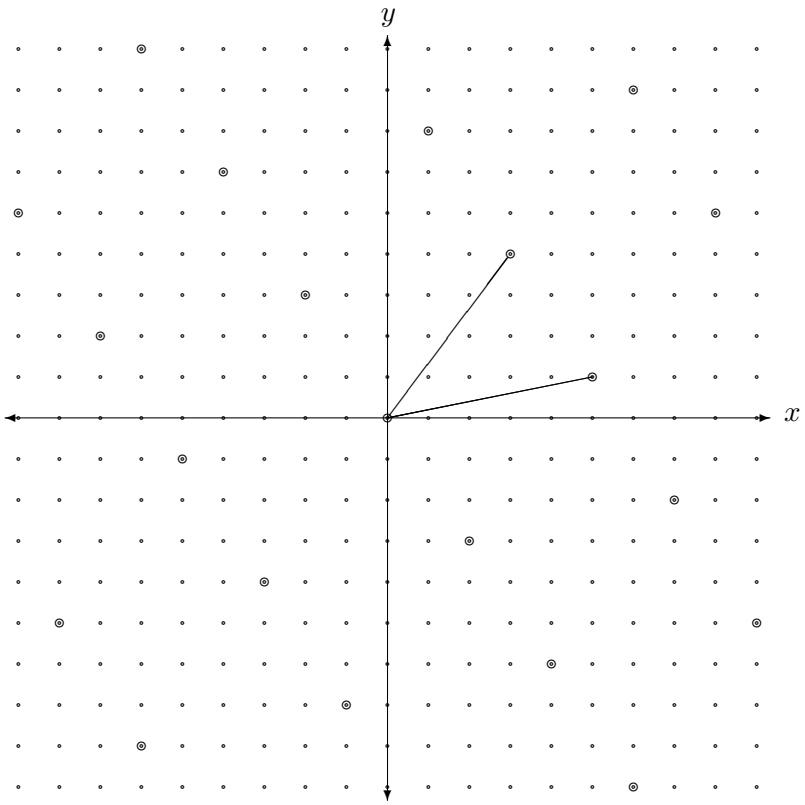


Figure 1.2: A lattice with basis $(5, 1)$, $(3, 4)$

Theorem 1.2.27. *Let L be a full lattice in $\mathbb{R}^n$. Then $\mathrm{vol}(L)$ is independent of the choice of basis. If $V = \{v_1, \cdots, v_n\} \subset L$ is any linearly independent set of vectors in L, then $D_V \neq 0$ and it is an integral multiple of $\mathrm{vol}(L)$. Moreover, $D_V = \mathrm{vol}(L)$ if and only if V is a basis of L.*

Proof. Let $U = \{u_1, \cdots, u_n\}$ be a basis of L. Then each v_i can be written as an integer linear combination of the u_j. This gives a matrix S with integer entries such that $M_V = SM_U$. The determinant of S is an integer so $D_V = |\det(S)|D_U$ is an integral multiple of D_U. If V is also a basis of L then we similarly obtain a matrix T with integer entries such that $M_U = TM_V$. This implies $TS = I$ so the determinants of S and T are integers with integer inverses, hence $|\det(S)| = 1$ and $D_U = D_V$. This proves the first two statements.

For the last statement, suppose $U \subset L$ and $V \subset L$ are collections of n linearly independent vectors, suppose U is a basis of L, and suppose $D_V = D_U$. We claim that V is also a basis of L. As above, write $V = SU$ where S is a matrix of integers. Then $\det(V) = \det(S)\det(U)$ so

$\det(S) = \pm 1$. By Cramer's rule, the inverse of S consists of rational numbers whose denominators are $\det(S)$, so S^{-1} also has integer entries. Hence, the equation $U = S^{-1}V$ expresses the u_i as integer linear combinations of the v_j, so V is also a basis for L. □

The proof of the following fact about lattice bases may be found in [3] Lemma 1, Section 2.6.

Theorem 1.2.28. *Let $L \subset K \subset \mathbb{R}^n$ be full lattices. Then K/L is a finite Abelian group. Let $u_1, \cdots, u_n$ and $v_1, \cdots, v_n$ be bases of L and K respectively. Each u_i is an integer linear combination of the vectors v_i, say, $u_i = A_{i1}v_1 + \cdots + A_{in}v_n$. Then the matrix $A = (A_{ij})$ has integer entries and $|K/L| = |\det(A)|$.* □

In a lattice, linear dependence over $\mathbb{R}$ implies linear dependence over $\mathbb{Z}$.

Lemma 1.2.29. *Let $u_1, \cdots, u_k$ be a set of vectors in $\mathbb{R}^n$ that is linearly independent over $\mathbb{R}$. Let v be a vector in the $\mathbb{Z}$-span of $u_1, \cdots, u_k$ and suppose that v is in the $\mathbb{R}$-span of $u_1, \cdots, u_\ell$ with $\ell \leq k$. Then v is in the $\mathbb{Z}$-span of $u_1, \cdots, u_\ell$*

Proof. Write $v = a_1u_1 + \cdots + a_ku_k$ with each $a_i \in \mathbb{Z}$, and $v = b_1u_1 + \cdots + b_\ell u_\ell$ with each $b_i \in \mathbb{R}$. By the uniqueness of the representation of a vector as a linear combination of a set of linearly independent vectors over a field, we have $a_1 = b_1, a_2 = b_2, \cdots, a_\ell = b_\ell$ and $a_{\ell+1} = \cdots = a_k = 0$. □

For any positive real number r, let $B_r(x) \subset \mathbb{R}^n$ denote the (closed) ball of radius r, centered at $x \in \mathbb{R}^n$. A subset $L \subset \mathbb{R}^n$ is *discrete* if for every x, r the set $B_r(x) \cap L$ is finite.

Theorem 1.2.30. *Every lattice $L \in \mathbb{R}^n$ is discrete.*

Proof. Any lattice is contained in a full lattice, so we may assume L is full, say with basis $u_1, \cdots, u_n$. Define $f : \mathbb{R}^n \to \mathbb{R}^n$ by $f(a_1u_1 + \cdots + a_nu_n) = (a_1, a_2, \cdots, a_n)$. Then f maps the lattice L isomorphically to the standard lattice $\mathbb{Z}^n \subset \mathbb{R}^n$ consisting of vectors with integer coordinates. For any x, r the image $f(B_r(x))$ is compact, hence closed and bounded, so it is contained in some n-cube with integer vertices and with edges of some (possibly very large) integer length, D. Such a cube contains $(D+1)^n$ integer vertices. Therefore $B_r(x)$ contains no more than $(D+1)^n$ lattice points in L. □

We leave as an exercise the proof that every discrete $\mathbb{Z}$-module in $\mathbb{R}^n$ is a lattice. This provides an alternate characterization of lattices that is sometimes used in the literature as definition. Although we will not need to use it, we state for completeness the following theorem of Minkowski,

Theorem 1.2.31. *Let $L \subset \mathbb{R}^n$ be a full lattice and let $X \subset \mathbb{R}^n$ be a bounded convex subset that is centrally symmetric. If $\mathrm{vol}(X) > 2^n \mathrm{vol}(L)$ then X contains a nonzero element of L.*

Sometimes a module M over a ring R has the structure of a commutative ring. If the function $a \mapsto a \cdot 1_M$ is a ring homomorphism, then we say that M is a (commutative) *S-algebra*. For example, every commutative ring is a $\mathbb{Z}$-algebra. If R is a subring of a ring R', then R' is an R-algebra. If R is commutative ring and S is a multiplicative set in R, then $S^{-1}R$ is an R-algebra. More generally, if I is an ideal of R and R/I is a subring of a ring R', then R' is an R-algebra.

1.2.l Inverse limits

The notions of directed system and inverse limit provide a powerful mechanism for studying infinite sequences.

Definition 1.2.32. *Let R be a ring and let $(P, \prec)$ be a partially ordered set. A* directed system of modules over R indexed by P *is a set of modules $\{M_r : r \in P\}$ and, for each pair $p, q \in P$ with $p \prec q$, a homomorphism $\mu_{q,p} : M_q \to M_p$. If $p \prec q \prec r$, then we must have $\mu_{r,p} = \mu_{q,p} \circ \mu_{r,q}$.*

If $\{M_r : r \in P\}$ is a directed system of modules over R indexed by P, then let the inverse limit of the system be

$$\varprojlim M_r = \varprojlim \{M_r : r \in P\} = \left\{ z \in \prod_{r \in P} M_r : \text{ if } p \prec q, \text{ then } \mu_{q,p}(z_q) = z_p \right\}.$$

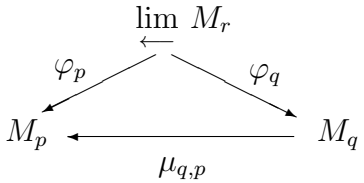
Here z_p denotes the pth component of $z \in \prod_{r \in P} M_r$.

Theorem 1.2.33. *The set $\varprojlim M_r$ is a module. For each $q \in P$ there is a homomorphism*

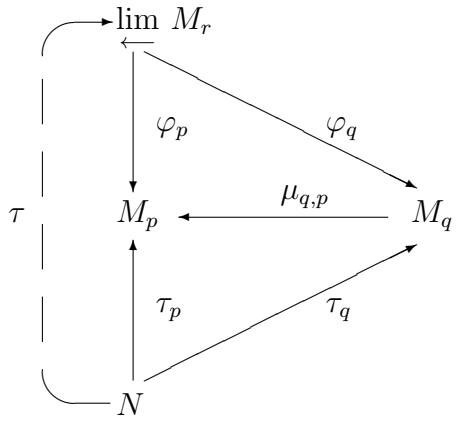
$$\varphi_q : \varprojlim M_r \to M_p$$

so that $\varphi_p = \mu_{q,p} \circ \varphi_q$ whenever $p \prec q$.

That is, the following diagram commutes.



If N is any R-module and $\{\tau_p : p \in P\}$ is a set of homomorphisms such that $\tau_p = \mu_{q,p} \circ \tau_q$ whenever $p \prec q$, then there is a unique homomorphism $\tau : N \to \varprojlim M_r$ so that $\tau_p = \varphi_p \circ \tau$. That is, the following diagram can be completed to a commutative diagram.



If also the M_p's are R-algebras and the homomorphisms $\mu_{q,p}$ are R-algebra homomorphisms, then $\varprojlim M_r$ is an R-algebra

Proof. Any Cartesian product $\prod_{r\in P} M_r$ of R-modules is an R-module, and $\varprojlim M_r$ is a subset that is closed under addition and scalar multiplication, so is also an R-module. The function φ_p is simply the restriction of the projection on M_p to $\varprojlim M_r$. The commutativity of the first diagram follows from the constraint on the elements of $\varprojlim M_r$.

If N and $\{\tau_p\}$ are as in the second condition and $a \in N$, then we define $\tau(a)$ to be the element of $\prod_{r\in P} M_r$ whose rth component is $\tau_r(a)$. That $\tau(a) \in \varprojlim M_r$ follows from the commutativity of the τ_r and the $\mu_{q,p}$. It is immediate that the second diagram commutes and that τ is unique.

The extension to R-algebras is straightforward. □

In the language of category theory, $\varprojlim M_r$ is a universal object for the directed system $\{M_r : r \in P\}$. This theorem often allows simple proofs that certain rings defined by different infinite constructions are isomorphic.

1.3 Characters and Fourier transforms

The Fourier transform can be defined in tremendous generality. In this section we describe the main properties of the Fourier transform for finite Abelian groups.

1.3.a Basic properties of characters

Definition 1.3.1. *A (complex)* character *of an Abelian group G is a group homomorphism from G to the multiplicative group $\mathbb{C}^\times = \mathbb{C} - \{0\}$ of the complex numbers. That is, it is a function $\chi : G \to \mathbb{C}$ such that $\chi(a+b) = \chi(a)\chi(b)$ for all $a, b \in G$. Such a character is* nontrivial *if $\chi(a) \neq 1$ for some a. The trivial character is denoted 1, and the collection of all characters of G is denoted $\widehat{G}$.*

The group operation in an Abelian group is usually denoted "+", and this can lead to some confusion since a character takes values in a multiplicative group. In particular, if χ is a character of G then $\chi(mg) = \chi(g)^m$ (for any integer m), and $\chi(0) = 1$. For example, if $G = \mathbb{Z}/(2)$ then there is a unique nontrivial character χ and it converts $\{0,1\}$ sequences into $\{\pm 1\}$ sequences. If G is a finite Abelian group then $|\chi(g)| = 1$ for all $g \in G$ (since $\chi(g)^{|G|} = 1$) so χ takes values in the set $\mu_{|G|}$ of roots of unity. It follows that $\chi(-g) = \overline{\chi}(g)$ (complex conjugate) for all $g \in G$.

The set of characters $\widehat{G}$ of a group G is itself a group with group operation defined by

$$(\chi_1 \cdot \chi_2)(a) = \chi_1(a)\chi_2(a)$$

and with the trivial character as identity. If $G = \mathbb{Z}/(N)$ is the additive group of integers modulo N then the group $\widehat{G}$ of characters is also cyclic and is generated by the primitive character $\chi(k) = e^{2\pi i k/N}$ for $k \in \mathbb{Z}/(N)$. If $G = G_1 \times G_2$ is a product of two groups then $\widehat{G} = \widehat{G}_1 \times \widehat{G}_2$. Specifically, if χ is a character of G then there are unique characters χ_1, χ_2 of G_1, G_2 (respectively) such that $\chi(g_1, g_2) = \chi_1(g_1)\chi_2(g_2)$, namely $\chi_1(g_1) = \chi(g_1, 1)$ and $\chi_2(g_2) = \chi(1, g_2)$ (for any $g_1 \in G_1$ and $g_2 \in G_2$). From this, together with the fundamental theorem for finite Abelian groups 1.1.16, it follows that the collection $\widehat{G}$ of characters of a finite Abelian group G is itself a finite Abelian group which is isomorphic to G. (The corresponding statement for infinite Abelian groups is false: for example, any nonzero $x \in \mathbb{C}$ defines a character of the integers $\mathbb{Z}$ by setting $\chi(m) = x^m$.)

Proposition 1.3.2. *Let G be a finite Abelian group, let $\chi : G \to \mathbb{C}^\times$ be a character, and let $g \in G$. Then*

$$\sum_{h \in G} \chi(h) = \begin{cases} 0 & \text{if } \chi \neq 1 \\ |G| & \text{if } \chi = 1 \end{cases} \tag{1.9}$$

and

$$\sum_{\psi \in \widehat{G}} \psi(g) = \begin{cases} 0 & \text{if } g \neq 0 \\ |G| & \text{if } g = 0. \end{cases} \tag{1.10}$$

Proof. If χ is nontrivial, there exists $a \in G$ with $\chi(a) \neq 1$. Then

$$\chi(a) \sum_{h \in G} \chi(h) = \sum_{h \in G} \chi(ah) = \sum_{h' \in G} \chi(h')$$

so

$$(1-\chi(a))\sum_{h\in G}\chi(g)=0.$$

For the second statement, note that g determines a character ψ_g of $\widehat{G}$ by the equation $\psi_g(\chi)=\chi(g)$. This character is nontrivial precisely when $g\neq 0$. In this case, the sum is $\sum_{\chi\in\widehat{G}}\psi_g(\chi)$, which is zero by the first part of the lemma. □

Corollary 1.3.3. *If G is a finite Abelian group and if $g,h\in G$ with $g\neq h$, then there exists a character χ such that $\chi(g)\neq\chi(h)$.*

Proof. If $\chi(g-h)=1$ for every $\chi\in\widehat{G}$, then summing over all characters gives $|G|$. By equation (1.10) we conclude that $g-h=0$. □

Corollary 1.3.4. *(Orthogonality relations) If G is a finite Abelian group and if $\psi,\chi\in\widehat{G}$ are distinct characters then*

$$\sum_{g\in G}\psi(g)\overline{\chi}(g)=0. \tag{1.11}$$

If $g,h\in G$ are distinct elements then

$$\sum_{\chi\in\widehat{G}}\chi(g)\overline{\chi}(h)=0. \tag{1.12}$$

Proof. The first equation follows by applying Proposition 1.3.2 to the character $\psi\chi^{-1}$. The second equation is $\sum_\chi\chi(g-h)=0$, also by Proposition 1.3.2. □

1.3.b Fourier transform

Let G be a finite Abelian group and $f:G\to\mathbb{C}$ be a function. Its *Fourier transform* $\widehat{f}:\widehat{G}\to\mathbb{C}$ is defined by

$$\widehat{f}(\chi)=\sum_{g\in G}\chi(g)f(g).$$

There are three standard properties of the Fourier tranform. First, the *inversion formula*

$$f(g)=\frac{1}{|G|}\sum_{\chi\in\widehat{G}}\widehat{f}(\chi)\overline{\chi}(g) \tag{1.13}$$

expresses an arbitrary function f as a linear combination of characters, so in particular, the characters span the group $\mathbb{C}[G]$ of complex-valued functions on G. Equation (1.13) follows immediately

from the orthogonality relation for characters, for the sum on the right hand side is

$$\frac{1}{|G|}\sum_{\chi\in\widehat{G}}\sum_{h\in G} f(h)\chi(h)\overline{\chi}(g) = \frac{1}{|G|}\sum_{h\in G} f(h)\sum_{\chi\in\widehat{G}}\chi(h-g) = f(g)$$

by equation (1.10). Second, the *convolution formula*

$$\widehat{f}\cdot\widehat{h} = \widehat{f*h} \tag{1.14}$$

expresses the product of $\widehat{f},\widehat{h}$ as the Fourier transform of the *convolution*

$$(f*h)(y) = \sum_{g\in G} f(g)h(y-g).$$

Finally, *Parseval's formula* says that for any function $f: G\to\mathbb{C}$,

$$|G|\sum_{g\in G}|f(g)|^2 = \sum_{\chi\in\widehat{G}}|\widehat{f}(\chi)|^2. \tag{1.15}$$

To see this, multiply $\widehat{f}(\chi)=\sum_g \chi(g)f(g)$ by its complex conjugate, $\sum_h \overline{\chi}(h)\overline{f}(h)$ to get

$$\sum_{\chi}|\widehat{f}(\chi)|^2 = \sum_{\chi}\sum_{g}\sum_{h} f(g)\overline{f}(h)\chi(g)\overline{\chi}(h) = \sum_{g,h} f(g)\overline{f}(h)\sum_{\chi}\chi(g)\overline{\chi}(h).$$

The inner sum vanishes unless $g=h$, which leaves $|G|\sum_g f(g)\overline{f}(g)$ as claimed.

If $G\cong\mathbb{Z}/(N)$ is a cyclic group then a choice $\zeta\in\mathbb{C}$ of primitive N-th root of unity determines an isomorphism $G\cong\widehat{G}$ which takes 1 to the character χ_1 with $\chi_1(k)=\zeta^k$. The other nontrivial characters χ_m are powers of this: $\chi_m(k)=\zeta^{mk}$. If $f: G\to\mathbb{C}$ is a function, its Fourier transform $\widehat{f}$ may be considered as a function $\widehat{f}: G\to\mathbb{C}$ by writing $\widehat{f}(m)$ rather than $\widehat{f}(\chi_m)$. Thus

$$\widehat{f}(m) = \sum_{k=0}^{N-1}\zeta^{mk}f(k). \tag{1.16}$$

Finally we remark that throughout this section, it is possible to replace the complex numbers $\mathbb{C}$ with any field K, provided K contains $|G|$ distinct solutions to the equation $x^{|G|}=1$. No changes to any of the proofs are needed; see Section 2.2.h. The resulting function $\widehat{f}$ is defined on all K-valued characters $\chi: G\to K^\times$. If K is a finite field then $\widehat{f}$ is called the *discrete Fourier transform*.

A generalized discrete Fourier transform is applicable when $x^{|G|}-1$ has repeated roots in K.

1.4 Polynomials

In this section we describe some of the basic properties of the ring of polynomials. The polynomial ring is among the most fundamental algebraic constructions. It is needed for much of the analysis of shift register sequences.

1.4.a Polynomials over a ring

Throughout this section R denotes a commutative ring. A *polynomial over* R is an expression

$$f = f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_d x^d = \sum_{i=0}^{d} a_i x^i$$

where $a_0, a_1, \cdots, a_d \in R$ and x is an indeterminate. The a_i are called the *coefficients of* R. When writing polynomials we may omit terms whose coefficients equal zero. We may also write the terms in a different order. If $a_d \neq 0$, then we say that $f(x)$ has degree $d = \deg(f(x))$. In this case a_d is called the *leading coefficient* of $f(x)$. We say $\deg(0) = -\infty$. If $\deg(f(x)) = 0$ then $f(x)$ is a *constant polynomial*. If $a_d = 1$ then $f(x)$ is *monic*. The term a_0 is called the *constant term*. The value of $f(x)$ at an element $b \in R$ is $f(a) = \sum_{i=0}^{d} a_i b^i$. An element $a \in R$ is a *root of* $f(x)$ if $f(a) = 0$. If $g(x) = \sum_{i=0}^{e} b_i x^i$ is a second polynomial over R, then we define

$$(f+g)(x) = f(x) + g(x) = \sum_{i=0}^{\max(d,e)} (a_i + b_i) x^i$$

(where we may have to extend one of the polynomials with zero coefficients so that this makes sense) and

$$(fg)(x) = f(x)g(x) = \sum_{i=0}^{d+e} \left(\sum_{j=\max(0,i-e)}^{\min(d,i)} a_j b_{i-j} \right) x^i.$$

The set of polynomials over R is denoted $R[x]$. The operations of addition and multiplication make $R[x]$ into a ring whose zero is the polynomial with every $a_i = 0$, and whose identity is the polynomial with $a_0 = 1$ and $a_i = 0$ for $i \geq 1$. The proof of the following lemma is straightforward.

Lemma 1.4.1. *If* $f(x), g(x) \in R[x]$, *then* $\deg(f+g) \leq \max(\deg(f), \deg(g))$ *with equality if* $\deg(f) \neq \deg(g)$. *Also,* $\deg(fg) \leq \deg(f) + \deg(g)$, *and equality can fail only when the product of the leading coefficients of* f *and* g *equals zero. In particular, if* R *is an integral domain then so is* $R[x]$.

If R is an integral domain, then the units in $R[x]$ are exactly the polynomials with degree zero and whose constant terms are units of R. This is false in general. For example, if $R = \mathbb{Z}/(4)$, then $(1+2x)^2 = 1$, so $1+2x$ is a unit with degree one. The following result says that sometimes we can perform division with remainder in $R[x]$.

Theorem 1.4.2. *(Division Theorem for polynomials)*
Let $f(x), g(x) \in R[x]$. Suppose the leading coefficient of g is a unit in R. Then there exist unique polynomials $q, r \in R[x]$ such that $\deg(r) < \deg(g)$ and

$$f(x) = q(x)g(x) + r(x).$$

Proof. By induction on the degree d of f. If $\deg(f) < \deg(g)$, take $q = 0$ and $r = f$. Otherwise, suppose f has leading coefficient a_d. Suppose g has degree $e \leq d$ and leading coefficient b_e. Then we have $f(x) = a_d b_e^{-1} x^{d-e} g(x) + f'(x)$ for some polynomial f'. The degree of f' is less than the degree of f, so by induction we have $f' = q'g + r$. It follows that $f = (a_d b_e^{-1} + q')x^{d-e}g + r$. For uniqueness, suppose $f = q_1 g + r_1 = q_2 g + r_2$ with $\deg(r_i) < \deg(g)$. Then $0 = (q_1 - q_2)g + (r_1 - r_2)$. The leading coefficient of g is invertible, and $\deg(r_1 - r_2) < \deg(g)$. It follows that the leading coefficient of $q_1 - q_2$ is zero, that is, $q_1 - q_2 = 0$. Therefore $r_1 - r_2 = 0$. □

Corollary 1.4.3. *If R is a field then $R[x]$ is a Euclidean domain with $\delta(f) = \deg(f)$.*

Theorem 1.4.4. *If a is a root of $f(x) \in R[x]$, then there exists a polynomial $q(x) \in R[x]$ such that*

$$f(x) = (x - a)q(x).$$

If R is an integral domain, then the number of distinct roots of f is no more than the degree of f (but see exercise 16).

Proof. Use the division theorem (Theorem 1.4.2) with $g = x - a$. The remainder r has degree zero but has a as a root. Thus r is zero. If R is an integral domain and if $b \neq a$ is another root of $f(x)$ then b is necessarily a root of $q(x)$. So the second statement follows by induction. □

The following theorem completes the proof of Theorem 1.2.14.

Theorem 1.4.5. *Suppose R is a GCD ring and a factorization domain. Then $R[x]$ is a factorization domain.*

Proof. We claim that every $f \in R[x]$ can be factored into a product of irreducibles. First we show that every $f \in R[x]$ has an irreducible divisor. Suppose not, and let d be the smallest degree of an element $f \in R[x]$ that has no irreducible divisor. Since R is a factorization domain, $d > 0$. Moreover, f is reducible. That is, $f = gh$ with neither g nor h a unit. The elements g and h

have no irreducible divisors since such a divisor would be a divisor of f as well. In particular, $\deg(h) > 0$. But then $\deg(g) < \deg(f)$ since R is an integral domain and this contradicts the minimality of $\deg(f)$.

Now let f be any element in $R[x]$. We already know that if f has degree zero, then it has an irreducible factorization, so let f have positive degree. Let a be the greatest common divisor of the coefficients of f and let $g = f/a$. If g has an irreducible factorization, then we obtain an irreducible factorization of f by multiplying those of g and a. Thus we may assume that the greatest common divisor of the coefficients of f is 1.

Now we use induction on the degree of f. If f has degree 1, then it is irreducible since no non-unit of R divides f other than an associate of f. If f has degree greater than 1, then by the first paragraph of this proof f has an irreducible divisor h. But h has positive degree so f/h has degree less than $\deg(f)$. By induction f/h has an irreducible factorization. Multiplying this by h gives an irreducible factorization of f. □

A root a of polynomial f is said to be *simple* if a is not a root of $f(x)/(x-a)$.

Lemma 1.4.6. *Let $q = \sum_{i=0}^{m} q_i x^i \in R[x]$ be a polynomial with coefficients in R. Consider the following statements*

1. *q_0 is invertible in R.*
2. *The polynomial x is invertible in the quotient ring $R[x]/(q)$.*
3. *The polynomials $q(x)$ and x are relatively prime in the ring $R[x]$.*
4. *There exists an integer $T > 0$ such that $q(x)$ is a factor of $x^T - 1$.*
5. *There exists an integer $T > 0$ such that $x^T = 1$ in the ring $R[x]/(q)$.*

Then statements (1), (2), and (3) are equivalent and if they hold, then

$$x^{-1} = -q_0^{-1}(q_1 + q_2 x + \cdots + q_m x^{m-1})$$

in $R[x]/(q)$. Statements (4) and (5) are equivalent (and the same T works for both) and $x^{-1} = x^{T-1}$ in $R[x]/(q)$. Statement (4) (or (5)) implies (1), (2), and (3). If R is finite then (1) (or (2) or (3)) implies (4),(5).

Proof. The statements are all straightforward except (possibly) the last one. Suppose that R is finite. Then the quotient ring $R[x]/(q)$ also contains finitely many elements so the powers $\{x^n\}$ of x in this ring cannot all be different. Hence there exists T such that $x^{n+T} \equiv x^n \pmod{q}$ for all sufficiently large n. Under assumption (2) this implies that $x^T \equiv 1 \pmod{q}$. In other words, q divides the polynomial $x^T - 1$, as claimed. □

When condition (4) (or (5)) in Lemma 1.4.6 holds, the smallest T such that $q(x)|(x^T - 1)$ is called the *order* of the polynomial q. This is admittedly confusing terminology since, in the

language of group theory, the order of the polynomial q is the order of x in the group $(R[x]/(q))^\times$. If condition (4) does not hold, then one may say that q does not have an order, or that its order is infinite. (For example, if $R = \mathbb{Q}$ the polynomial $q(x) = x - 2$ has infinite order.)

The following theorem will be useful when we discuss roots of unity.

Theorem 1.4.7. *Let a and b be positive integers. Then over any ring R the polynomial $x^a - 1$ divides $x^b - 1$ if and only if a divides b.*

Proof. By the Division Theorem for integers, we can write $b = qa + r$ with $0 \leq r < a$. Then

$$x^b - 1 = (x^{b-a} + x^{b-2a} + \cdots + x^r)(x^a - 1) + x^r - 1.$$

Sine $\deg(x^r - 1) < \deg(x^a - 1)$, it follows that $x^a - 1$ divides $x^b - 1$ if and only if $x^r - 1 = 0$. This holds if and only if $r = 0$, hence if and only if a divides b. □

1.4.b Polynomials over a field

Theorem 1.4.8. *If F is a field, then $F[x]$ is Euclidean with $\delta(f) = \deg(f)$. Every ideal in $F[x]$ has a unique monic principal generator. Any $f(x) \in F[x]$ can be written in the form*

$$f(x) = ap_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$$

where $a \in F$, the p_i are distinct monic irreducible elements of $F[x]$, and the e_i are positive integers. This representation is unique apart from changing the order of the p_i.

Proof. It follows from Theorem 1.4.2 that $F[x]$ is Euclidean. It is also principal and is a UFD by Theorem 1.2.14. Each irreducible polynomial has a unique monic associate (divide by the leading coefficient). This accounts uniquely for a. □

It also follows from Theorem 1.2.14 that $F[x]$ is a GCD ring, but to be precise we have the following theorem.

Theorem 1.4.9. *Let F be a field and $f_1, \cdots, f_k \in F[x]$, not all zero. There is a unique monic $g \in F[x]$ such that (1) g divides every f_i and (2) if h divides every f_i then h also divides g. Moreover, g can be written in the form*

$$g = h_1 f_1 + h_2 f_2 + \cdots + h_k f_k \tag{1.17}$$

for some $h_1, h_2, \cdots, h_k \in F[x]$.

Proof. Let $I = \{h_1 f_1 + h_2 f_2 + \cdots + h_k f_k : h_1, h_2, \cdots, h_k \in F[x]\}$. Then I is an ideal in $F[x]$, so by Theorem 1.4.8, I has a unique monic generator g. Since $g \in I$, g can be written in the form in equation (1.17). It follows that any h that divides every f_i also divides g. Since $f_i \in I$, g divides f_i. □

We write $g = \gcd(f_1, \cdots, f_k)$. It can be found by the usual Euclidean algorithm by repeatedly using Theorem 1.4.2. There is also a notion of least common multiple in $F[x]$. The following theorem later allows us to construct finite fields of all possible sizes. The proof is omitted.

Theorem 1.4.10. *If F is a finite field and d is a positive integer, then there is at least one irreducible polynomial of degree d in $F[x]$.*

If $F \subseteq E$ are fields and if $a \in E$ is an element that is the root of some polynomial with coefficients in F, then we say a is *algebraic over F*. A polynomial $f \in F[x]$ is called a *minimal polynomial* of a (over F) if it is monic, if $f(a) = 0$ and if it is a polynomial of smallest degree with these properties.

Theorem 1.4.11. *Suppose a is algebraic over F. Then it has a unique minimal polynomial $f \in F[x]$. The minimal polynomial f is also the unique monic irreducible polynomial in $F[x]$ having a as a root. If $g \in F[x]$ is any other polynomial such that $g(a) = 0$ then f divides g in $F[x]$.*

Proof. If two monic polynomials $f, g \in F[x]$ have the same (minimal) degree and both have a as a root then $f - g$ has smaller degree, which is a contradiction. If f is a minimal polynomial of a and $f = gh$, then $0 = f(a) = g(a)h(a)$ so $g(a) = 0$ or $h(a) = 0$. By the minimality of f, whichever factor has a as a root must have the same degree as f, so f is irreducible.

Now suppose f is a monic irreducible polynomial such that $f(a) = 0$. The set

$$J = \{h \in F[x] : \ h(a) = 0\}$$

is an ideal, so it is principal. It contains f, but f is irreducible, so $J = (f)$ is the ideal generated by f, and f is the unique monic polynomial with this property. If $g(a) = 0$ then $g \in J$ so g is a multiple of f. In particular, f is the minimal polynomial of a. □

More generally, we can think consider the "operator" on rings that takes a ring R to the polynomial ring $R[x]$. Strictly speaking this is not a function since there is no set of all rings. Rather, it is a (covariant) functor on the category of rings. We shall not, however pursue these notions in this book.

1.5 Exercises

1. Prove that if G_1 and G_2 are groups, then the direct product $G_1 \times G_2$ is a group. Prove that $G_1 \times G_2$ is Abelian if G_1 and G_2 are Abelian.

2. Describe the set of all subgroups of the group $\mathbb{Z}/m\mathbb{Z}$.

3. Let $\varphi : G \to H$ be a group homomorphism. Prove that $\mathrm{Ker}(\varphi)$ is a subgroup of G and $\mathrm{Im}(\varphi)$ is a subgroup of H.

4. Let G be a group and let H be a subgroup of G. Prove that the relation defined by $a \sim b$ if there is an $h \in H$ such that $b = ah$ is an equivalence relation. Find an example where the definition $aHbH = abH$ does not make the set of equivalence classes into a group.

5. Prove that a subgroup H of a group G is normal if and only if for every $a \in G$ and $h \in H$, we have $aha^{-1} \in H$.

6. Theorem 1.1.15: Let $\varphi : G \to G'$ be a homomorphism.

   a. Prove that $\mathrm{Ker}(\varphi)$ is normal in G.
   b. Prove that the quotient $G/\mathrm{Ker}(\varphi)$ is isomorphic to $\mathrm{Im}(\varphi)$.
   c. Conversely, prove that if H is a normal subgroup of G, then the map $a \mapsto aH$ is a surjection from G to G/H with kernel equal to H.

7. Show that the set of endomorphisms of an Abelian group is a ring.

8. Theorem 1.2.7:

   a. Suppose $\varphi : R \to S$ is a ring homomorphism. Prove that $\mathrm{Ker}(\varphi)$ is an ideal of R and φ induces an isomorphism between $R/\mathrm{Ker}(\varphi)$ and the image of f.
   b. Prove that if I is an ideal of R, then the map $a \mapsto a + I$ is a homomorphism from R onto R/I with kernel I.

9. Prove that a GCD ring with no infinite chain of proper ascending ideals is also a LCM (least common multiple) ring.

10. Let $\{R_s : s \in S\}$ be a family of rings. Prove that R_S is the unique (up to isomorphism) ring such that if T is any ring and $\psi_s : T \to R_s$ any set of homomorphisms, then there is a homomorphism $g : T \to R_S$ such that $\psi_s = \varphi_s \circ g$ for every $s \in S$.

11. Prove that if V is a vector space over a field F, then for every $u \in V$ we have $0 \cdot u = 0$.

12. Theorem 1.2.21:

   a. Prove that every vector space has a basis. (Hint: use Zorn's Lemma.)
   b. Prove that if S is a basis for a vector space V, then every vector can be written uniquely as a linear combination of elements of S.

13. Prove by induction on the dimension that every discrete $\mathbb{Z}$-module in $\mathbb{R}^n$ is a lattice.

14. Let $f(x) = a_0 + a_1 x + \cdots + a_d x^d \in \mathbb{C}[x]$ be a polynomial and let $F : \mathbb{Z} \to \mathbb{C}$ be the function $F(i) = a_i$ (and $F(i) = 0$ if $i < 0$ or $i > d$). Let $g(x) = b_0 + b_1 x + \cdots + b_e x^e$ and let $G : \mathbb{Z} \to \mathbb{C}$ be the corresponding function. Show that the product $f(x)g(x)$ polynomial corresponds to the convolution $F * G$.

15. Develop a theory of characters as functions with values in an arbitrary field F rather than $\mathbb{C}$. For certain parts you will need to assume that F contains the n-th roots of unity.

16. Let $R = \mathbb{Z} \times \mathbb{Z}$. Let $f(x) = (1, 0)x - (1, 0) \in R[x]$. Show that f has infinitely many roots in the ring R.

Chapter 2 Fields

Fields are rings where every nonzero element is a unit. Many sequence generators can be viewed as implementing multiplication by a fixed element in a ring. Since finite fields have cyclic groups of units, they provide a source of large period sequence generators. In Section 2.1 we describe the Galois theory of field extensions. In Sections 2.2 and 2.4 we study in some detail two important classes of fields – finite fields, which give us a way to make algebraic constructions with finite alphabets, and algebraic number fields, which generalize the field of rational numbers. In Section 2.5 we describe local fields. These are fields that are complete with respect to a notion of convergent sequences. Elements of these fields can sometimes be viewed as infinite sequences over some alphabet. We also study quadratic forms, which are the source of several important constructions of sequences with good correlation properties (see Section 2.3).

2.1 Field extensions

In this section we summarize (without proofs) some standard facts about field extensions.

2.1.a Galois group

If F is a field and E is a ring, then the kernel of any nonzero homomorphism $F \to E$ is the zero ideal (the only proper ideal), so every homomorphism is an injection. We say that E is an *extension* of F. Elements of E can then be added and multiplied by elements of F so E becomes a vector space over F. The dimension of E as a vector space over F is called the *degree* or the *dimension* of the extension.

A field R is *algebraically closed* if every polynomial $p(x) \in F[x]$ factors completely, $p(x) = k(x-a_1)(x-a_2)\cdots(x-a_n)$ where $\deg(p) = n$ and where $k, a_i \in F$. Every field F is contained in an algebraically closed field $\overline{F}$ of finite degree over F, called an *algebraic closure* of F.

If G is a subgroup of the group of automorphisms of a field E, then the set of elements in E that are fixed by every automorphism in G (that is, $\sigma(a) = a$ for every $a \in E$ and every $\sigma \in G$) is denoted E^G. It is necessarily a field since it is closed under addition, multiplication, and inverse. If $F \subset E$ are fields then the group $\mathrm{Aut}_F(E)$ of automorphisms of E which fix each element of F is the *Galois group* of E over F and it is denoted by $\mathrm{Gal}(E/F)$. If $G = \mathrm{Gal}(E/F)$, then $F \subseteq E^G$. If in fact $F = E^G$, then we say that E *is a Galois extension of* F . The discovery of Galois extensions by Evariste Galois was a turning point in the understanding of the nature of algebraic equations and triggered a great transformation in the way mathematics was done.

If $F \subset E$ is a finite extension of fields and if $\overline{F}$ is an algebraic closure of F then there are finitely many embeddings $h_1, \cdots, h_n : E \to \overline{F}$. If E is a Galois extension of F then these embeddings all have the same image. In this case, a choice of one embedding (say, h_1) determines a one to one correspondence $h_i \leftrightarrow \sigma_i$ with elements of the Galois group $\mathrm{Gal}(E/F)$ by $h_i(x) = h_1(\sigma_i(x))$.

Proposition 2.1.1. *Let $F \subset E$ be a finite extension and let $T : E \to F$ be a nonzero F-linear map. Then for any F-linear map $f : E \to F$ there exists a unique element $a \in E$ such that $f(x) = T(ax)$ for all $x \in E$.*

Proof. The field E has the structure of a vector space over F, of some finite dimension, say, n. Then $\mathrm{Hom_F(E, F)}$ is the dual vector space and it also has dimension n. Each $a \in E$ gives an element $f_a \in \mathrm{Hom_F(E, F)}$ by $f_a(x) = T(ax)$ which is also nonzero unless $a = 0$. So the association $a \mapsto f_a$ gives a mapping $E \to \mathrm{Hom_F(E, F)}$ which is a homomorphism of n dimensional vector spaces, whose kernel is 0. Therefore it is an isomorphism. □

2.1.b Trace and norm

Let E be an extension of degree $n < \infty$ of a field F. Choose a basis $e_1, e_2, \cdots, e_n$ of E as a vector space over F. Each $a \in E$ defines a mapping $L_a : E \to E$ by $L_a(x) = ax$. This mapping is E-linear, hence also F-linear, so it can be expressed as an $n \times n$ matrix M_a with respect to the chosen basis. If $a \neq 0$ then the matrix M_a is invertible. The *trace*, $\mathsf{Tr}_F^E(a)$ and *norm* $\mathsf{N}_F^E(a)$ are defined to be the trace and determinant (respectively) of the matrix M_a. It is common to write $\mathsf{Tr}(a) = \mathsf{Tr}_F^E(a)$ and $\mathsf{N}(a) = \mathsf{N}_F^E(a)$ if the fields E and F are understood.

Theorem 2.1.2. *Let $F \subset E$ be a finite extension of fields.*

1. *For all $a, b \in E$ and $c \in F$ we have $\mathsf{Tr}(a + b) = \mathsf{Tr}(a) + \mathsf{Tr}(b)$ and $\mathsf{Tr}(ca) = c\mathsf{Tr}(a)$. That is, Tr is F-linear.*
2. *For all $a, b \in E$ we have $\mathsf{N}(ab) = \mathsf{N}(a)\mathsf{N}(b)$ so $\mathsf{N}_F^E : E^\times \to F^\times$ is a homomorphism of multiplicative groups. It is surjective.*
3. *If $F \subset L \subset E$ are finite extensions then for all $a \in E$,*
$$\mathsf{Tr}_F^L(\mathsf{Tr}_L^E(a)) = \mathsf{Tr}_F^E(a) \quad \text{and} \quad \mathsf{N}_F^L(\mathsf{N}_L^E(a)) = \mathsf{N}_F^E(a).$$
4. *If E is a Galois extension of F then $\mathsf{Tr}_F^E : E \to F$ is nonzero and*
$$\mathsf{Tr}_F^E(a) = \sum_{\sigma \in \mathrm{Gal}(E/F)} \sigma(a) \quad \text{and} \quad \mathsf{N}_F^E = \prod_{\sigma \in \mathrm{Gal}(E/F)} \sigma(a).$$

Parts (1) and (2) are straightforward. We omit the proofs (see [20], [3]) of parts (3) and (4) but we will return to the trace and norm in Section 2.2 and Section 2.4. There are situations in which the trace $\mathsf{Tr}_F^E : E \to F$ is the zero map, but if E, F are finite fields or if $\mathrm{char}(E) = 0$ or if E is a Galois extension of F then the trace is not zero.

2.2 Finite fields

In this section we analyze the structure of finite fields, or *Galois fields*. For a more complete treatment see the excellent reference by Lidl and Niedereitter [21]. Our first task is to identify all finite fields and all inclusion relations among them.

2.2.a Basic properties

Theorem 2.2.1. *Let p be a prime number. For each $d > 0$ there is (up to isomorphism) a unique field $\mathbb{F}_{p^d}$ with p^d elements. These account for all finite fields. If $e > 0$ is another integer, then there is an inclusion $\mathbb{F}_{p^d} \subseteq \mathbb{F}_{p^e}$ if and only if d divides e. That is, the (combinatorial) lattice of finite fields with characteristic p under inclusion is isomorphic to the lattice of whole numbers under divisibility. The subfield $\mathbb{F}_{p^d}$ consists of those elements a of $\mathbb{F}_{p^e}$ satisfying $a^{p^d} = a$.*

The field $\mathbb{F}_{p^d}$ is sometimes denoted $GF(p^d)$ (for "Galois field"). The proof of Theorem 2.2.1 will occupy the rest of Section 2.2.a.

Suppose d is a positive integer and F is a finite field with r elements. Let $f(x)$ be an irreducible polynomial over F with degree d. Then by Theorem 1.2.5.4, $F[x]/(f(x))$ is a field. It has r^d elements. In particular, if p is a prime integer and we take $F = \mathbb{Z}/(p)$, then this together with Theorem 1.4.10 shows that there exists a finite field of order p^d for every prime p and positive integer d.

Next suppose F is a finite field with characteristic $p > 0$. Recall that we showed in Theorem 1.2.8 that p is prime. It follows that the mapping $\mathbb{Z}/(p) \to F$ which takes an element n to $1 + 1 + \cdots + 1$ (n times) is a ring homomorphism. So we can view $\mathbb{Z}/(p)$ as a subfield of F. Hence F has the structure of a finite dimensional vector space over $\mathbb{Z}/(p)$. By Theorem 1.2.22, F has p^d elements for some d.

Proposition 2.2.2. *If $F \subseteq E$ are two finite fields, then E and F have the same characteristic. If p is the characteristic, then $|F| = p^d$ and $|E| = p^e$ for some integers d and e such that d divides e.*

Proof. If F has characteristic p and E has characteristic r, then $|F| = p^d$ and $|E| = r^e$ for some d and e. But E is a vector space over F, so $r^e = (p^d)^k$ for some k. Thus $r = p$ and $e = dk$. □

To complete the picture of the set of finite fields we want to show that there is, up to isomorphism, a unique finite field of a given cardinality. First we need a lemma.

Lemma 2.2.3. *If F is a finite field, then every $a \in F$ is a root of the polynomial $x^{|F|} - x$ and we have*

$$x^{|F|} - x = \prod_{a \in F} (x - a).$$

No other element of any extension field of F is a root of this polynomial.

Proof. The multiplicative group of F has order $|F|-1$, so by Theorem 1.1.3 any nonzero element $a \in F$ satisfies $a^{|F|-1} = 1$. Therefore any element $a \in F$ satisfies $a^{|F|} = a$. That is, every a is a root of the polynomial $x^{|F|} - x$. It follows that $x - a$ divides $x^{|F|} - x$. Furthermore, the degree of $x^{|F|} - x$ equals $|F|$, so there are no other roots of this polynomial in E. The factorization follows from Theorem 1.4.4. □

Corollary 2.2.4. *Suppose E is a field, p is a prime number, and d is a positive integer. Then E contains at most one subfield of order p^d.*

Proof. Suppose F is a subfield of E of order p^d. By Lemma 2.2.3 every $a \in F$ is a root of $x^{p^d} - x$, and there are no other roots of this polynomial in E.

Now suppose F' is another subfield of E of order p^d. The same reasoning applies to F'. Thus $F = F'$. □

Proposition 2.2.5. *Let p be a prime number and let $d > 0$ be an integer. Any two finite fields with p^d elements are isomorphic.*

Proof. Let $E = (\mathbb{Z}/(p))[x]/(f(x))$, where $f(x)$ is an irreducible polynomial with degree d and coefficients in $\mathbb{Z}/(p)$. It is enough to show that any field F with p^d elements is isomorphic to E.

By Lemma 2.2.3, every $a \in E$ satisfies $a^{p^d} = a$. In particular, $x^{p^d} - x = 0$ in E, so $f(x)$ divides $x^{p^d} - x$ as polynomials. That is, $x^{p^d} - x = f(x)g(x)$ for some $g(x) \in (\mathbb{Z}/(p))[x]$.

On the other hand, we can think of $x^{p^d} - x$ as a polynomial over F. By the same reasoning, every element of F is a root of this polynomial, so

$$f(x)g(x) = x^{p^d} - x = \prod_{a \in F} (x - a).$$

In particular, $f(x)$ factors into linear factors over F. Let a be a root of $f(x)$ in F. If the elements $\{1, a, a^2, \cdots, a^{d-1}\}$ were linearly dependent over $(\mathbb{Z}/(p))[x]$, a would be a root of a lower degree polynomial, and this polynomial would divide $f(x)$. That would contradict the irreducibility of $f(x)$. Thus they are linearly independent and hence a basis (F has dimension d over $(\mathbb{Z}/(p))[x]$). That is, every b in F can be written

$$b = \sum_{i=0}^{d-1} c_i a^i,$$

with $c_i \in (\mathbb{Z}/(p))[x]$. We define a function

$$L\left(\sum_{i=0}^{d-1} c_i a^i\right) = \sum_{i=0}^{d-1} c_i x^i$$

from F to E. This function is one-to-one and it can be checked that it preserves multiplication and addition. Hence it is an isomorphism. □

Thus for each prime power $q = p^d$ there is a unique field $\mathbb{F}_q$ with q elements.

Proposition 2.2.6. *Let p be prime and let d, e be positive integers. Then the field $F = \mathbb{F}_{p^d}$ may be realized as a subfield of $E = \mathbb{F}_{p^e}$ if and only if d divides e. In this case it is the set*

$$F = \left\{ x \in E : \ x^{p^d} = x \right\}.$$

Proof. If F is a subfield of E then E is a vector space over F, of some dimension k. Consequently $|E| = |F|^k$ so $e = dk$. To prove the converse, assume $e = dk$ for some positive integer k. Let $q = p^d = |F|$. Recall from Lemma 2.2.3 that E consists of the distinct roots of the polynomial $x^{p^e} - x = x^{q^k} - x$. This polynomial is divisible by the polynomimal $x^q - x$, for the quotient is

$$x^{(q^k-1)-(q-1)} + x^{(q^k-1)-2(q-1)} + \cdots + x^{q-1} + 1.$$

Thus E contains a set S of q distinct roots of the polynomial $(x^q - x)$. By Lemma 1.2.9, both addition and multiplication commute with raising to the qth power, so the subset $S \subset E$ is a field. Therefore it is isomorphic to the field $F = \mathbb{F}_q$. □

Suppose $f \in F[x]$ is irreducible. Recall that in the terminology of Section 1.4.a, the order of f is the smallest T such that $f(x)|(x^T - 1)$. This is the order of x in the group of units of $F[x]/(f)$, a group that has $|F|^{\deg(f)} - 1$ elements. Thus by Theorem 1.1.3 the order of f divides $|F|^{\deg(f)} - 1$.This completes the proof of Theorem 2.2.1.

2.2.b Galois groups of finite fields

Some of the preceding notions can be understood in terms of Galois groups (see Section 2.1.a). Let $E = \mathbb{F}_{p^e}$ where p is prime. By Lemma 1.2.9 the mapping $\sigma : E \to E$, $\sigma(x) = x^p$ is a field automorphism, meaning that it is additive, multiplicative, and invertible. However $\sigma^e(x) = x^{p^e} = x$ so $\sigma^e = I$ is the identity. Thus the various powers of σ (including $\sigma^0 = I$) form a cyclic group of automorphisms, of order e, which fix each element of $\mathbb{F}_p$.

Proposition 2.2.7. *The group $\{\sigma^0 = I, \sigma, \cdots, \sigma^{e-1}\}$ is the Galois group* $\mathrm{Gal}(E/\mathbb{F}_p)$.

Proof. The Galois group $\mathrm{Gal}(E/F)$ is the set of automorphisms of E that fix each element of F. So it suffices to show that any automorphism $\tau : E \to E$ is some power of σ. Let f be an irreducible polynomial over $\mathbb{F}_p$ with degree e, and let a be a root of f. Then $\mathbb{F}_{p^d} = \mathbb{F}_p[a]$ and $1, a, a^2, \cdots, a^{e-1}$ is a basis for $\mathbb{F}_{p^e}$ over $\mathbb{F}_p$. Thus to show that two automorphisms are equal, it suffices to show that they are equal on a. We have that $\sigma^i(f) = f$ for every i, so $\sigma^i(a)$ is a root of f. Similarly, $\tau(a)$ is a root of f. The $\sigma^i(a)$ are distinct – otherwise a and hence $\mathbb{F}_{p^e}$ are in a proper subfield, which is a contradiction. Thus there are $e = \deg(f)$ of them, and they account for all the roots of f. In particular, $\tau(a) = \sigma^i(a)$ for some i. So $\tau = \sigma^i$, proving the proposition. □

Theorem 2.2.8. *Let $F = \mathbb{F}_{p^d} \subset E = \mathbb{F}_{p^e}$ be finite fields. Then the Galois group* $\mathrm{Gal}(E/F)$ *is a cyclic subgroup group of* $\mathrm{Gal}(E/\mathbb{F}_p)$*, of order e/d. It is generated by the automorphism $\sigma^d : x \mapsto x^{p^d}$. The field $F \subset E$ consits of those elements of E that are fixed by every element of* $\mathrm{Gal}(E/F)$ *(which is the same as being fixed by the generator σ^d). Consequently the field E is a* Galois extension *of the field F.*

Proof. It follows from Proposition 2.2.6 that F is the subfield of E that is fixed by σ^d. So the various powers of σ^d are contained in $\mathrm{Gal}(E/F)$. By Proposition 2.2.7, every automorphism of F is some power of σ. But d is the smallest power of σ that fixes F because the equation $x^{p^k} = x$ has at most p^k solutions. Consequently $\mathrm{Gal}(E/F)$ consists of all powers of σ^d. These elements form a cyclic subgroup of $\mathrm{Gal}(E/\mathbb{F}_p)$ of order e/d. □

Thus we have an inclusion reversing correspondence between the lattice of subfields of $\mathbb{F}_{p^d}$ and the lattice of subgroups of $\mathrm{Gal}(\mathbb{F}_{p^d}/\mathbb{F}_p)$. The main theorem of Galois theory describes the solutions of a polynomial equation in terms of the Galois group.

Theorem 2.2.9. *Let F be a finite field with q elements and let $f(x) \in F[x]$ be a polynomial of degree d with coefficients in F. Let E be an extension field of F and suppose $\alpha \in E$ is a root of f. Then for any $\sigma \in Gal(E/F)$, the element $\sigma(\alpha) \in E$ is also a root of f. If f is irreducible in $F[x]$ and if E is the degree d extension of F then all the roots of f are contained in E. They consist exactly of the Galois conjugates,*

$$\sigma_i(\alpha) = \alpha^{q^i},$$

where $0 \leq i \leq d-1$. That is, where σ_i ranges over all elements of $Gal(E/F)$.

Proof. Let $q = |F|$. The Galois group $Gal(E/F)$ is cyclic and it is generated by the mapping $\sigma : E \to E$ given by $\sigma(a) = a^q$. If $f(x) = \sum_{i=0}^{d} a_i x^i$ and if $\alpha \in E$ is a root of f, then

$$0 = \sigma(f(\alpha)) = \left(\sum_{i=0}^{d} a_i \alpha^i \right)^q = \sum_{i=0}^{d} a_i^q \alpha^{iq} = \sum_{i=0}^{d} a_i \sigma(\alpha) = f(\sigma(\alpha))$$

(by Lemma 1.2.9), so $\sigma(\alpha)$ is also a root of f.

Now suppose f is irreducible and, without loss of generality, monic. Then it is the minimal polynomial of α by Theorem 1.4.11. But the polynomial

$$g(x) = \prod_{\tau \in Gal(E/F)} (x - \tau(\alpha)) \in E[x]$$

has the same degree as f, and it is fixed under each element of $Gal(E/F)$. So $g \in F[x]$, and it has α as a root. Therefore $g = f$, so the roots of f are all the Galois conjugates of α. □

2.2.c Primitive elements

To work within a particular finite field F, it is useful to have some structural information. An element $a \in F$ is called *primitive* if every nonzero element of F can be written as a power of a. A polynomial $f \in \mathbb{F}_p[x]$ of degree d is primitive if it is irreducible and if one (and hence all) of its roots in $\mathbb{F}_{p^d}$ are primitive elements.

Lemma 2.2.10. *Let $F = \mathbb{F}_q$ be the field with q elements. Let $f \in F[x]$ be a polynomial. Then f is primitive if and only if its order is $q^{\deg(f)} - 1$.*

Proof. In the ring $F[x]/(f)$ the element x is a root of the polynomial $f(x)$. If x is primitive then the order of x is $T = |F| - 1 = q^{\deg(f)} - 1$. Thus T is the smallest integer such that $x^T = 1 \pmod f$, which is to say that T is the smallest integer such that f divides $x^T - 1$. Thus the order of f is T. The converse is similar. □

We next show that every finite field has primitive elements. This implies that the multiplicative group of a finite field is cyclic.

Proposition 2.2.11. *The finite field $\mathbb{F}_{p^d}$ has $\phi(p^d - 1)$ primitive elements.*

Proof. Suppose that $a \in \mathbb{F}_{p^d}$ has order e. That is, $a^e = 1$ and no smaller positive power of a equals 1. Then the elements $1, a, a^2, \cdots, a^{e-1}$ are distinct and are all roots of $x^e - 1$. That is,

$$x^e - 1 = (x-1)(x-a)(x-a^2)\cdots(x-a^{e-1}).$$

It follows that every element whose eth power equals 1 is a power of a, and an element $b = a^i$ has order e if and only if $\gcd(i, e) = 1$. Thus if there is at least one element of order e, then there are exactly $\phi(e)$. That is, for every e there are either 0 or $\phi(e)$ elements of order e.

Furthermore, by Lemma 2.2.3 every nonzero $a \in F$ is a root of the polynomial $x^{p^d-1} - 1$. Thus if there is an element in F with order e, then e divides $p^d - 1$. By Lemma 1.2.10, for any positive integer k

$$\sum_{e|k} \phi(e) = k.$$

Thus we have

$$\begin{aligned} p^d - 1 &= \sum_{e|p^d-1} |\{a \in F : \text{ the order of } a = e\}| \\ &\leq \sum_{e|p^d-1} \phi(e) = p^d - 1. \end{aligned}$$

Therefore the two sums are equal. Since each term in the first sum is less than or equal to the corresponding term in the second sum, each pair of corresponding terms must be equal.

In particular, the number elements with order $p^d - 1$ equals $\phi(p^d - 1) > 0$. □

In fact, it can be shown that every finite field $\mathbb{F}_{p^d}$ has a *primitive normal basis* over a subfield $\mathbb{F}_{p^c}$. This is a basis of the form $a, a^{p^c}, \cdots, a^{p^{d-c}}$ with a primitive. The interested reader can find the details in [21, Section 2.3].

2.2.d Roots of unity

Let $N \in \mathbb{Z}$ be a positive integer. Over the complex numbers the polynomial $x^N - 1$ factors completely into distinct linear factors

$$x^N - 1 = \prod_{j=0}^{N-1} (x - \zeta^j)$$

where $\zeta \in \mathbb{C}$ is a primitive N-th root of unity, for example, $\zeta = e^{2\pi i/N}$. These N-th roots of unity form an Abelian group under multiplication, denoted μ_N, that is isomorphic to $\mathbb{Z}/(N)$. The field $\mathbb{Q}(\zeta)$ is called a *cyclotomic field*. It is a Galois extension of $\mathbb{Q}$ of degree $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \phi(n)$. The Galois group is Abelian and is isomorphic to $\mathbb{Z}/(N)^\times$. If $s \in \mathbb{Z}/(N)^\times$ is relatively prime to N then the corresponding element $\sigma_s \in \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ acts on $\mathbb{Q}(\zeta)$ by $\sigma_s(\zeta^k) = \zeta^{ks}$.

Lemma 2.2.12. *Let $\zeta \in \mathbb{C}$ be a primitive Nth root of unity and let $p(x) \in \mathbb{Q}[x]$ be a polynomial with rational coefficients. Suppose $|p(\zeta)|^2 \in \mathbb{Q}$ is a rational number. Then $|p(\zeta^s)|^2 = |p(\zeta)|^2$ for any integer s relatively prime to N with $1 \le s \le N-1$.*

Proof. Let $p(x) = a_0 + a_1 x + \cdots + a_d x^d$ with $a_i \in \mathbb{Q}$. Then $|p(\zeta)|^2 = p(\zeta)\overline{p(\zeta)} \in \mathbb{Q}$ is fixed under the action of the element $\sigma_s \in \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$, where $\overline{\zeta} = \zeta^{-1}$ denotes complex conjugation. Therefore

$$\begin{aligned} p(\zeta)\overline{p(\zeta)} &= \sigma_s\left(p(\zeta)\overline{p(\zeta)}\right) \\ &= (a_0 + a_1\zeta^s + \cdots + a_k\zeta^{ks})(a_0 + a_1\zeta^{-s} + \cdots + a_k\zeta^{-ks}) \\ &= p(\zeta^s)\overline{p(\zeta^s)} \end{aligned}$$

□

The situation is more complicated over a finite field. Let $F = \mathbb{F}_q$ be a finite field of characteristic p. Let $N \in \mathbb{Z}$ be a positive integer. Define d as follows. Write $N = p^e n$ where p does not divide n. Let $d = \mathrm{ord}_n(q)$. (In the group theoretic sense: the image of q in $\mathbb{Z}/(n)$ is invertible, and d is the least integer such that $q^d \equiv 1 \pmod{n}$, cf. Section 1.2.d.) The following theorem says that $x^N - 1$ factors completely in the extension field $\mathbb{F}_{q^d}$ of $\mathbb{F}_q$, but the roots are not distinct if $p^e > 1$.

Theorem 2.2.13. *Given N, q as above, there exists $\beta \in \mathbb{F}_{q^d}$ such that*

$$x^N - 1 = \prod_{i=0}^{n-1} (x - \beta^i)^{p^e}. \tag{2.1}$$

Moreover, $\mathbb{F}_{q^d}$ is the smallest extension of $\mathbb{F}_q$ over which $x^N - 1$ splits into linear factors.

Proof. Let $\alpha \in \mathbb{F}_{q^d}$ be a primitive element and let $\beta = \alpha^{(q^d-1)/n}$. Since $q^d \equiv 1 \pmod{n}$ the exponent $(q^d-1)/n$ is an integer. The powers $\beta^0, \beta^1, \cdots, \beta^{n-1} \in \mathbb{F}_{q^d}$ are distinct, and $\beta^n = 1$. Thus β is a primitive n-th root of unity, and $x^n - 1 = \prod_{i=1}^{n-1}(x - \beta^i)$. Equation (2.1) follows. The minimality of $\mathbb{F}_{q^d}$ is left as an exercise. □

The factors in equation (2.1) can be grouped together to give the factorization of $x^N - 1$ over the field $\mathbb{F}_q$. Let $\gamma = \beta^k \in \mathbb{F}_{q^d}$ be any root of $x^n - 1$. Then the remaining roots of the minimal polynomial of γ over $\mathbb{F}_q$ are $\{\gamma^{q^i} = \beta^{kq^i} : i \geq 0\}$. The set of exponents

$$C_k(q) = C_k = \{k, qk \pmod{n}, q^2k \pmod{n}, \cdots\}$$

is called the *kth cyclotomic coset modulo n relative to q* (the terms "modulo n" and "relative to q" may be omitted if n and/or q are understood). The minimal polynomial of γ is then the product

$$f_k(x) = \prod_{i \in C_k} (x - \beta^i).$$

If $C_{j_1}, \cdots, C_{j_m}$ are the distinct cyclotomic cosets in $\{0, 1, \cdots, n-1\}$, then they form a partition of $\{0, 1, \cdots, n-1\}$ and the desired factorizations are

$$x^n - 1 = \prod_{i=1}^{m} f_k(x) \quad \text{and} \quad x^N - 1 = \prod_{i=1}^{m} f_k(x)^{p^e}.$$

2.2.e Trace and norm on finite fields

Theorem 2.2.14. *Let $F = \mathbb{F}_q \subset E = \mathbb{F}_{q^n}$ be finite fields of characteristic p. Then the following statements holds.*

1. *The trace function $\mathsf{Tr}_F^E : E \to F$ is given by*

$$\mathsf{Tr}_E^F(a) = a + a^q + a^{q^2} + \cdots + a^{q^{n-1}} = \sum_{\sigma \in \mathrm{Gal}(\mathbb{E}/\mathbb{F})} \sigma(a). \tag{2.2}$$

2. *The norm is given by*

$$\mathsf{N}_F^E(a) = \prod_{\sigma \in \mathrm{Gal}(E/F)} \sigma(a) = a^{(q^n-1)/(q-1)} \in F.$$

3. *The trace is nonzero and for all $c \in F$, we have $|\{a \in E : \mathsf{Tr}(a) = c\}| = p^{e-d}$.*
4. *For all $0 \neq c \in F$ we have $|\{a \in E : \mathsf{N}(a) = c\}| = (|E|-1)/(|F|-1)$.*
5. *For all $a \in E$ we have $\mathsf{Tr}_F^E(a^p) = \mathsf{Tr}_F^E(a)^p$.*

6. $\mathsf{Tr}_F^E(1) \in \mathbb{F}_p$ *and* $\mathsf{Tr}_F^E(1) \equiv n \pmod{p}$.
7. *If* $L : E \to F$ *is an* F*-linear function, then there is an element* $a \in E$ *such that* $L(b) = \mathsf{Tr}(ab)$ *for all* $b \in E$.

Proof. 1. Verification of the second equality in equation (2.2) is left as an exercise. It follows that the quantity on the right side of equation (2.2), which we denote by $T(a)$, is fixed by each $\sigma \in \mathrm{Gal}(E/F)$ so it is indeed an element of F. Both maps T and Tr are F-linear, hence are equal if and only if they are equal on a basis. Let $a \in E$ be a root of an irreducible polynomial of degree n over F. Then the set $\{1, \alpha, \alpha^2, \cdots, \alpha^{n-1}\}$ forms a basis for E (over F). If the minimal polynomial for a is

$$f(x) = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} + x^n$$

then the matrix

$$M_a = \begin{pmatrix} 0 & 1 & \cdots & 0 & 0 \\ & & \vdots & & \\ 0 & 0 & \cdots & 1 & 0 \\ 0 & 0 & \cdots & 0 & 1 \\ -a_0 & -a_1 & \cdots & -a_{m-2} & -a_{m-1} \end{pmatrix} \tag{2.3}$$

is the corresponding *companion matrix*: it has 1 in each entry of the superdiagonal, $-a_0, \cdots, -a_{d-1}$ in the last row, and 0s elsewhere. The characteristic polynomial of the matrix M_a is exactly the polynomial $f(x)$, so the eigenvalues of M_a (i.e. the roots of its characteristic polynomial) are the Galois conjugates of a. So the trace of M_a is $-a_{n-1}$. On the other hand,

$$f(x) = \prod_{\sigma \in \mathrm{Gal}(E/F)} (x - \sigma(a)),$$

so $-a_{n-1} = \sum_{\sigma \in \mathrm{Gal}(E/F)} \sigma(a)$.

2. The same argument applies to the determinant of the matrix M_a, which is

$$(-1)^n a_0 = (-1)^{2n} \prod_{\sigma \in \mathrm{Gal}(E/F)} \sigma(a).$$

3. Thinking of E as an n-dimensional vector space over F, the mapping $\mathsf{Tr} : E \to F$ is linear, so its rank is either zero or 1. If the rank is zero then $\mathsf{Tr}(x) = 0$ for all $x \in E$, however this equation is a polynomial of degree q^{n-1} so it has at most $q^{n-1} < q^n$ solutions. Therefore $\mathsf{Tr} : E \to F$ is surjective so its kernel $K = \mathsf{Tr}^{-1}(0) \subset E$ is a vector subspace of dimension $n - 1$ which therefore contains q^{n-1} elements. For any $0 \neq a \in F$ the set $\mathsf{Tr}^{-1}(a)$ is a translate of K, that is, an affine subspace of the same dimension, which therefore contains the same number of elements.

4. The norm is a homomorphism $\mathsf{N}_F^E : E^\times \to F^\times$. If α is a primitive element in E, then

$$\mathsf{N}_F^E(\alpha) = \prod_{i=0}^{n-1} \alpha^{q^i} = \alpha^{\sum_{i=0}^{n-1} q^i} = \alpha^{(q^n-1)/(q-1)},$$

which is primitive in F. Thus N_F^E surjective so its kernel is a subgroup of order $(|E|-1)/(|F|-1)$.

5. All the operations used to define Tr commute with raising to the pth power.

6. We have $\mathsf{Tr}(1) = 1 + 1^q + \cdots + 1^{q^{n-1}} = 1 + 1 + \cdots + 1$, with n terms.

7. This is a special case of Proposition 2.1.1. □

2.2.f Quadratic equations in characteristic 2

Let $F = \mathbb{F}_{2^r}$ be a finite field of characteristic 2 and let $a, b, c \in F$ with $a \neq 0$. The trace function is a necessary ingredient for determining when the quadratic equation

$$ax^2 + bx + c = 0 \tag{2.4}$$

has a solution $x \in F$.

Theorem 2.2.15. *If $a, b \neq 0$ then the quadratic equation (2.4) has a solution $x \in F$ if and only if $\mathsf{Tr}_{\mathbb{F}_2}^F(ac/b^2) = 0$, in which case it has two distinct solutions. If $b = 0$ (and $a \neq 0$) then it has a unique solution.*

Proof. First consider the case $a = b = 1$. To solve the equation $x^2 + x = c$, consider the following sequence, where $\phi : F \to F$ is the linear map, $\phi(x) = x^2 - x = x^2 + x$,

$$0 \longrightarrow \mathbb{F}_2 \longrightarrow F \xrightarrow{\phi} F \xrightarrow{\mathsf{Tr}_{\mathbb{F}_2}^F} \mathbb{F}_2 \longrightarrow 0$$

Then this sequence is exact (see Definition 1.1.10): exactness at the first term is immediate and exactness at the fourth terms follows from Theorem 2.2.14. The kernel $\mathrm{Ker}(\phi) = \{0, 1\} = \mathbb{F}_2$ is 1-dimensional. It follows that the sequence is exact at the second term, and in particular, the mapping ϕ is two-to-one. Therefore the mapping ϕ has rank $r - 1$. But $\mathsf{Tr} : F \to \mathbb{F}_2$ is surjective so its kernel also has dimension $r - 1$. Since $\mathrm{Im}(\phi) \subset \mathrm{Ker}(\mathsf{Tr})$, and they have the same dimension, they must coincide. In other words, $c \in \mathrm{Ker}(\mathsf{Tr})$ if and only if $c = x^2 - x$ for some x, and in this case there are two such values of x.

	$Q(x,y)$	conditions	$N_v,\ v=0$	$N_v,\ v\neq 0$
Type I	xy	$b\neq 0,\ \mathsf{Tr}^F_{\mathbb{F}_2}(ac/b^2)=0$	$2q-1$	$q-1$
Type II	x^2	$b=0$	q	q
Type III	$h(x^2+y^2)+xy$	$b\neq 0,\ \mathsf{Tr}^F_{\mathbb{F}_2}(ac/b^2)=1$	1	q

Table 2.1: Quadratic forms in characteristic 2.

For the general case, the transformation

$$x=\frac{b}{a}y$$

converts equation (2.4) into the equation

$$\frac{b^2}{a}(y^2+y)=c$$

which therefore has a solution if and only if

$$\mathsf{Tr}^F_{\mathbb{F}_2}(ac/b^2)=0,$$

in which case it has two solutions. Finally, if $b=0$ then the equation $x^2=c/a$ has one solution because 2 is relatively prime to 2^r-1 so the mapping $F\to F$ given by $x\to x^2$ is invertible (and in fact it is an isomorphism of $\mathbb{F}_2$-vector spaces). □

Corollary 2.2.16. *Let $a,b,c\in F=\mathbb{F}_{2^r}$. Fix $h\in F$ with $\mathsf{Tr}^F_{\mathbb{F}_2}(h)=1$. Then the quadratic form*

$$Q(x,y)=ax^2+bxy+cy^2$$

can be transformed, using a linear transformation of variables, into one of the three quadratic forms in Table 2.1. The number N_v of solutions to the equation $Q(x,y)=v$ is also given.

Proof. The transformation $x\to\alpha x+\beta y$ changes Q into the quadratic form

$$a\alpha^2x^2+b\alpha xy+(a\beta^2+b\beta+c)y^2.$$

By Theorem 2.2.15 if $\mathsf{Tr}^F_{\mathbb{F}_2}(ac/b^2)=0$ then $\beta\in F$ can be chosen so that the coefficient of y^2 vanishes. Taking $\alpha=1/b$ leaves

$$Q=\frac{a}{b^2}x^2+xy.$$

Now the transformation

$$y \to \frac{a}{b^2}x + y$$

changes Q to xy. This is Type I.

If $\mathsf{Tr}_{\mathbb{F}_2}^F(ac/b^2) \neq 0$ then choose β so that $a\beta^2 + b\beta + c = b^2h^2/a$ (which is possible, by Theorem 2.2.15) and choose $\alpha = bh/a$. Then the transformation $x \to \alpha x + \beta y$ converts the quadratic form Q into the form

$$\frac{b^2h}{a}(hx^2 + xy + hy^2).$$

The further transformation

$$x \to \frac{\sqrt{a}}{b\sqrt{h}}x \quad \text{and} \quad y \to \frac{\sqrt{a}}{b\sqrt{h}}y$$

transforms Q into $hx^2 + xy + hy^2$. This is Type II. Finally, if $b = 0$ (and $a, c \neq 0$), use

$$x \to \frac{x + \sqrt{c}y}{\sqrt{a}}$$

to convert $Q(x, y)$ into x^2. This is Type III.

Counting the number N_v of solutions to $Q(x, y) = v$ is trivial for Types I and II. For Type III, if $v = 0$ then for any nonzero choice of y we need to solve for x in the equation $hx^2 + xy + hy^2 = 0$. Since $\mathsf{Tr}_{\mathbb{F}_q}^F(h) = 1$ this has no solutions. Thus $(0, 0)$ is the unique solution. If $v \neq 0$, imagine choosing y and solving for x, which will be possible if and only if $\mathsf{Tr}_{\mathbb{F}_2}^F(h^2y^2 - hv) = 0$. As y varies in F the quantity inside the trace varies among all elements of F, and $q/2$ of these have trace zero. For each such choice of y there are two distinct choices for x, for a total of q solutions. □

2.2.g Characters and exponential sums

Let F be a finite field, say, $|F| = q = p^r$ where p is a prime number. Let $F^\times$ be the group of all nonzero elements of F under multiplication and let F^+ be the group of all elements of F under addition. A character $\chi : F^+ \to \mathbb{C}^\times$ is called an *additive* character. If χ is a nontrivial additive character then every additive character is of the form $\psi(x) = \chi(Ax)$ for some element $A \in F$. (Different values of A give distinct characters, and there are $|F|$ of them, which therefore account for all additive characters.)

A character $\psi : F^\times \to \mathbb{C}^\times$ is called a *multiplicative* character of F. It is common to extend each multiplicative character $\psi : F^\times \to \mathbb{C}$ to all of F by setting $\psi(0) = 0$. If q is odd then the *quadratic character*

$$\eta(x) = \begin{cases} 1 & \text{if } x \text{ is a square} \\ -1 & \text{otherwise} \end{cases} \tag{2.5}$$

is a multiplicative character. If p is an odd prime and $0 \neq x \in \mathbb{F}_p$ then the *Legendre symbol* is

$$\left(\frac{x}{q}\right) = \eta(x).$$

Since the prime field $\mathbb{F}_p = \mathbb{Z}/(p)$ is cyclic, the additive group F^+ is isomorphic to the additive group $(\mathbb{Z}/(p))^r$, so we obtain from Section 1.3.b the notion of a Fourier transform $\widehat{f}$ of any function $f : F \to \mathbb{C}$, with respect to this additive group structure. Since the multiplicative group $F^\times$ is cyclic, we obtain a second notion of Fourier transform of any function $f : F^\times \to \mathbb{C}$. Equation (1.16) gives explicit formulae for these Fourier transforms. In this case they are sometimes called the Hadamard and Walsh transforms (respectively).

If ψ is a multiplicative character one can take its Fourier transform $\widehat{\psi}$ with respect to the additive structure to obtain the *Gauss sum*

$$\widehat{\psi}(\chi) = G(\psi, \chi) = \sum_{g \in F} \chi(g)\psi(g) = \sum_{g \in F^\times} \chi(g)\psi(g) \tag{2.6}$$

for any additive character χ. Conversely, equation (2.6) may be interpreted as the Fourier transform $\widehat{\chi}$ of the additive character χ evaluated on the multiplicative character ψ. The results in Section 1.3.b therefore give a number of simple facts concerning Gauss sums. In particular, the Fourier expansion of a multiplicative character ψ in terms of additive characters as in equation (1.13) gives

$$\psi(g) = \frac{1}{|F|} \sum_{\chi} G(\psi, \chi)\overline{\chi}(g) = \frac{1}{|F|} \sum_{\chi} G(\psi, \overline{\chi})\chi(g).$$

We state without proof the following classical *Gauss bound* and *Weil bound* (cf. [21] Section 5.2, Section 5.4) and its improvement by Carlitz and Uchiyama [4].

Theorem 2.2.17. *If χ, ψ are nontrivial additive and multiplicative $\mathbb{C}$-valued characters (respectively) of a finite field F then*

$$|G(\psi, \chi)| = \sqrt{|F|}.$$

Theorem 2.2.18. *Let $F = \mathbb{F}_{p^r}$ with p prime. Let $f \in F[x]$ be a polynomial of degree $n \geq 1$. Let χ be a nontrivial additive character of F. Suppose either (a) $\gcd(n, p) = 1$ or (b) f is not of the form $g^p - g + b$ where $g \in F[x]$ and $b \in F$. Then*

$$\left| \sum_{x \in F} \chi(f(x)) \right| \leq (n-1)\sqrt{|F|}. \tag{2.7}$$

Let ψ be a nontrivial multiplicative character of F of order $m > 1$ and let d be the number of distinct roots of f in its splitting field over F. Instead of assumptions (a) or (b) above, assume

that the monic polynomial $a^{-1}f$ (where a is the leading coefficient of f) is not the m-th power of a polynomial $g(x) \in F[x]$. Then

$$\left|\sum_{x\in F} \psi(f(x))\right| \leq (d-1)\sqrt{|F|}. \tag{2.8}$$

The following theorem of A. Weil [31], [29] combines all of the above.

Theorem 2.2.19. *Let $F = \mathbb{F}_q$ be a finite field. Let ψ be a nontrivial multiplicative character of order d. Let χ be a nontrivial additive character. Let $f(x), g(x) \in F[x]$ be polynomials with $n = \deg(g)$. Assume that $f(x)$ has m distinct roots in F, and further assume that $\gcd(d, \deg(f)) = \gcd(q, \deg(g)) = 1$. Then*

$$\left|\sum_{x\in F} \psi(f(x))\chi(g(x))\right| \leq (m+n-1)\sqrt{|F|}.$$

For polynomials in several variables there is the following bound of Deligne [6] (Theorem 8.4):

Theorem 2.2.20. *Let F be a finite field and let χ be a nontrivial additive character. Let $f(x_1, x_2, \cdots, x_n)$ be a polynomial of degree m. Assume m is relatively prime to $|F|$. Assume also that the homogeneous part of f of maximal degree ($= m$) is nonsingular, when it is considered as a form over the algebraic closure of F. Then*

$$\left|\sum_{x\in F^n} \chi(f(x))\right| \leq \left((m-1)\sqrt{|F|}\right)^n.$$

2.2.h The Discrete Fourier transform

While the (usual) Fourier transform involves complex valued functions, the discrete Fourier transform involves functions with values in a finite field F. It is defined in a manner completely analogous to equation (1.16), provided the field F contains all the required roots of unity. (For cyclic groups $G = \mathbb{Z}/(N)$, this assumption may be relaxed.)

Let G be a finite Abelian group and let $N \in \mathbb{Z}$ be its *characteristic*, that is, the smallest integer such that $0 = x + x + \cdots + x$ (N times) for all $x \in G$. (Then N divides $|G|$ and it is the order of the largest cyclic subgroup of G.) Let $F = \mathbb{F}_q$ be a finite field and suppose that N and q are relatively prime. Let $d = \mathrm{ord}_N(q)$ and let $E = \mathbb{F}_{q^d}$. By Theorem 2.2.13 the field E is the smallest field extension of F that contains all the N-th roots of unity. (In what follows, the field E may be replaced by any larger field.)

Continue to assume that $N = \mathrm{char}(G)$ and $\mathrm{char}(E)$ are relatively prime. The group of *discrete characters* $\widehat{G}$ is the set of (group) homomorphisms $\psi : G \to E^\times$. It forms a group under multiplication of characters, $(\chi\psi)(g) = \chi(g)\psi(g)$. If $G = \mathbb{Z}/(N)$ then $\widehat{G}$ is also cyclic of order N and is generated by the primitive character $\chi(x) = b^x$ where $b \in E$ is a primitive N-th root of unity. If $G = G_1 \times G_2$ then $\widehat{G} = \widehat{G}_1 \times \widehat{G}_2$. It follows that the group of characters $\widehat{G}$ is a finite Abelian group that is abstractly isomorphic to G and in particular that $|\widehat{G}| = |G|$. The proof of Proposition 1.3.2 works here too and we obtain the following.

Lemma 2.2.21. *Let G be a finite Abelian group characteristic N, $F = \mathbb{F}_q$, and $E = \mathbf{q^d}$ where $d = ord_N(q)$. Then the following hold.*

1. *If $\chi : G \to E^\times$ is a nontrivial character then $\sum_{g\in G} \chi(g) = 0$.*
2. *If $0 \neq g \in G$ then $\sum_{\chi\in\widehat{G}} \chi(g) = 0$.*
3. *If $g \neq h \in G$ then there exists $\chi \in \widehat{G}$ such that $\chi(g) \neq \chi(h)$.*
4. *If $\psi \neq \chi \in \widehat{G}$ then $\sum_{g\in G} \psi(g)\chi^{-1}(g) = 0$.*
5. *If $g \neq h \in G$ then $\sum_{\chi\in\widehat{G}} \chi(g)\chi^{-1}(h) = 0$.* □

With $G, F, E, \widehat{G}$ as above, for any $f : G \to E$ define its *Fourier transform* $\widehat{f} : \widehat{G} \to E$ by

$$\widehat{f}(\chi) = \sum_{g\in G} \chi(g)f(g).$$

Then the *convolution formula* (1.14) and the *Fourier inversion formula* (1.13) hold:

$$\widehat{f}\cdot\widehat{g} = \widehat{f * G} \quad \text{and} \quad f(g) = \frac{1}{|G|}\sum_{\chi\in\widehat{G}} \widehat{f}(\chi)\chi^{-1}(g)$$

with the same proof as in Section 1.3.b. The proof in Section 1.3.b gives a weak analog to Parseval's equation,

$$\sum_{\chi\in\widehat{G}} \widehat{f}(\chi)\widehat{f}(\chi^{-1}) = \sum_{g\in G} f(g)^2 \quad \text{and} \quad \sum_{\chi\in\widehat{G}} \widehat{f}(\chi)^2 = \sum_{g\in G} f(g)f(-g).$$

Although the discrete Fourier transform and the complex Fourier transform are entirely parallel in their definition and properties, there is no apparent relation between them.

If $G = \mathbb{Z}/(N)$, then a choice of primitive N-th root of unity $b \in E$ determines an isomorphism $G \cong \widehat{G}$ which takes $1 \in \mathbb{Z}/(N)$ to the character χ_1 with $\chi_1(k) = b^k$. The other characters are powers of this one: $\chi_m(k) = b^{mk}$. If $f : \mathbb{Z}/(N) \to E$ is a function, then its discrete Fourier transform may be considered as a function $\widehat{f} : \mathbb{Z}/(N) \to E$ by writing $\widehat{f}(m)$ rather than $\widehat{f}(\chi_m)$. In other words,

$$\widehat{f}(m) = \sum_{k=0}^{N-1} b^{mk} f(k) \quad \text{and} \quad f(g) = \frac{1}{N}\sum_{m=1}^{N-1} \widehat{f}(m)b^{-mg}.$$

2.3 Quadratic forms over a finite field

2.3.a Quadratic forms and their classification

The standard reference for this section is Lidl and Niederreiter's book on finite fields [21]. Let $F = \mathbb{F}_q$ be a finite field with q elements. A quadratic form in n variables over F is a polynomial $Q(x_1, x_2, \cdots, x_n)$ in n variables such that each term has degree two, that is,

$$Q(x_1, \cdots, x_n) = \sum_{i=1}^{n} \sum_{j=1}^{n} a_{ij} x_i x_j.$$

It follows that $Q(cx) = c^2 Q(x)$ for any $c \in F$. If q is odd then the function $Q(x)$ may be expressed as $Q(x) = x^t A x$ where A is the symmetric matrix $A_{ij} = \frac{1}{2}(a_{ij} + a_{ji})$ for $i \neq j$ and $A_{ii} = a_{ii}$. Consequently there is an associated bilinear form $B(x, y) = x^t A$ (here we are thinking of the vectors x and y as column vectors).

If q is even then every quadratic form Q may be expressed as $Q(x) = x^t A x$ where the matrix A is not necessarily symmetric, and where the transpose matrix A^t gives the same quadratic form. If $M : F^n \to F^n$ is an invertible $n \times n$ matrix representing a linear change of coordinates, then the matrix of the quadratic form with respect to the new coordinates is $M^t A M$. In particular, the determinant of A changes by the factor $\det(M)^2$.

The *rank* of a quadratic form Q is the smallest integer m such that there exists a linear change of variables $(x_1, \cdots, x_n) \to (y_1, \cdots, y_n)$ so that the resulting quadratic form involves only the variables $y_1, y_2, \cdots, y_m$. A quadratic form in n variables is *nondegenerate* if its rank is n. If $Q : F^n \to F$ is a quadratic form then there exists a *maximal nondegenerate subspace* that is, a subspace $V \subset F^n$ such that $\dim(V) = \text{rank}(Q)$ and so that Q restricted to V is nondegenerate. A vector $w \in F^n$ is in the *kernel* of Q if $Q(w + x) = Q(x)$ for all $x \in F^n$. The kernel of Q is a vector subspace of F^n and it is complementary to any maximal nondegenerate subspace $V \subset F^n$, meaning that $V \cap W = \{0\}$ and $V + W = F^n$.

If F is a field of characteristic 2 then every element is a square. But if the characteristic of F is odd then half the elements are squares, and the *quadratic character* $\eta : F^\times \to \{0, 1\}$ is defined by $\eta(x) = 1$ if $x = a^2$ for some $a \in F$ and $\eta(x) = -1$ otherwise. (It is customary to define $\eta(0) = 0$ as this convention can often be used to simplify various formulae.) Denote by $\Delta(Q)$ the determinant of the restriction of Q to a maximal nondegenerate subspace; it is well defined up to multiplication by a square in $\mathbb{F}$. If $\text{rank}(Q) = m$ define

$$\Delta'(Q) = \begin{cases} (-1)^{m/2}\Delta(Q) & \text{if } m \text{ is even,} \\ (-1)^{(m-1)/2}\Delta(Q) & \text{if } m \text{ is odd.} \end{cases} \tag{2.9}$$

If the characteristic of F is odd, the properties of the quadratic form Q depend on whether or not the element $\Delta'(Q) \in F$ is a square, that is, whether $\eta(\Delta'(Q))$ is $+1$ or -1.

The following theorem gives the classification of quadratic forms over the finite field $F = \mathbb{F}_q$ of arbitrary characteristic. Although the proofs are not difficult, they are tedious and they can be found in [21]. (See Theorem 2.2.15 for the case $m = 2$ and characteristic 2.) In this classification, the symbol B_m denotes the quadratic form

$$B_m(x_1, \cdots, x_n) = x_1x_2 + x_3x_4 + \cdots + x_{m-1}x_m. \tag{2.10}$$

Theorem 2.3.1. ([21] Thm 6.30) *Suppose Q is a quadratic form of rank m in $n \geq m$ variables over a field $F = \mathbb{F}_q$. If q is even, fix an element $h \in F$ such that $\mathsf{Tr}_{\mathbb{F}_2}^F(h) = 1$. Then there is a linear change of variables so that Q is one of the quadratic forms listed in Table 2.2.*

		q **even**
Type I	(m even)	$Q(x) = B_m(x)$
Type II	(m odd)	$Q(x) = B_{m-1}(x) + x_m^2$
Type III	(m even)	$Q(x) = B_{m-2}(x) + x_{m-1}x_m + h(x_{m-1}^2 + x_m^2)$

q **odd**
$Q(x) = a_1x_1^2 + a_2x_2^2 + \cdots + a_mx_m^2$, $a_i \neq 0$

Table 2.2: Classification of quadratic forms over $\mathbb{F}_q$

(If q is odd and if $b \in F$ is a fixed non-square then $Q(x)$ can even be reduced to one of the two quadratic forms $Q(x) = x_1^2 + \cdots + x_{m-1}^2 + ax_m^2$ where $a = 1$ or $a = b$, but for most purposes the above diagonal form suffices.)

2.3.b Solutions to $Q(x) + L(x) = u$

Let F be a finite field. In this section we wish to count the number of solutions to the equation $Q(x) + L(x) = u$ where $Q : F^n \to F$ is a quadratic form and $L : F^n \to F$ is a linear mapping. This calculation is the central step in determining the cross-correlation of m-sequences, geometric sequences, GMW sequences, and Gold sequences. In order to simplify the presentation we define the following function $\nu : F \to \{-1, q-1\}$ by

$$\nu(x) = \begin{cases} -1 & \text{if } x \neq 0 \\ q-1 & \text{if } x = 0 \end{cases}$$

With $\Delta'(Q) = \pm\Delta(Q)$ as defined in equation (2.9), the following theorem counts the number of solutions to the equation $Q(x) = u$. The proof is not difficult but it is tedious and it will be omitted. We use the convention that $\eta(0) = 0$.

Theorem 2.3.2. ([21] Thm. 6.26, 6.27, 6.31) *Let Q be a quadratic form of rank m in n variables over a field $F = \mathbb{F}_q$. Let $u \in F$. Then the number N of solutions to the equation $Q(x_1, x_2, \cdots, x_n) = u$ is given in Table 2.3.*

	q **even**	
Type I	(m even)	$N = q^{n-1} + \nu(u)q^{n-1-m/2}$
Type II	(m odd)	$N = q^{n-1}$
Type III	(m even)	$N = q^{n-1} - \nu(u)q^{n-1-m/2}$

q **odd**	
(m odd)	$N = q^{n-1} + \eta(u)\eta(\Delta')q^{n-(m+1)/2}$
(m even)	$N = q^{n-1} + \nu(u)\eta(\Delta')q^{n-1-m/2}$

Table 2.3: Number of solutions to $Q(x) = u$

We now use this result to describe the number of solutions $x \in F^n$ of the equation

$$Q(x) + L(x) = u \tag{2.11}$$

where Q is a quadratic form and L is a linear function. We first show that the case $\text{rank}(Q) < n$ can be reduced to the case when Q has maximal rank, then we count the number of solutions to (2.11) assuming Q has maximal rank. The answer shows, in particular, that if $Q \neq 0$ then the function $Q(x) + L(x)$ cannot be identically zero.

Proposition 2.3.3. *Let $F = \mathbb{F}_q$ be a finite field, let $Q : F^n \to F$ be a quadratic form with $m = \text{rank}(Q) < n$ and let $L : F^n \to F$ be a nonzero (hence, surjective) linear mapping. Let $V \subset F^n$ be a maximal subspace on which Q is nondegenerate. Then the number N_u of solutions to the equation $Q(x) + L(x) = u$ is*

$$N_u = \begin{cases} q^{n-1} & \text{if } \text{Ker(Q)} \not\subset \text{Ker(L)} \\ q^{n-m}N'_u & \text{if } \text{Ker(Q)} \subset \text{Ker(L)} \end{cases}$$

where N'_u is the number of solutions x to equation (2.11) with $x \in V$.

Proof. This follows immediately from the direct sum decomposition $F^n \cong \text{Ker(Q)} \oplus \text{V}$ and the fact that L can be written as the sum of a linear function L_1 on Ker(Q) and a linear function L_2 on V. □

Theorem 2.3.4. *Let $u \in \mathbb{F}_q$. Let $Q : \mathbb{F}_q^m \to \mathbb{F}_q$ be one of the standard quadratic forms of (maximal) rank m listed in the classification, Theorem 2.3.1. Let $L(x) = \sum_{i=1}^m c_i x_i$ be a linear function. Let $N = N_u$ denote the number of elements $x \in \mathbb{F}_q^m$ so that $Q(x) + L(x) = u$. Then N_u is given in Table 2.4, where $\tau(c,u) = 0$ if $c_m = 0$, otherwise*

$$\tau(c,u) = (-1)^{\mathsf{Tr}_{\mathbb{F}_2}^F\left(\frac{u+B_{m-1}(c)}{c_m^2}\right)} = \pm 1; \tag{2.12}$$

and where $R = R(Q,c)$ is given in equation (2.13).

	q **even**	
Type I	(m even)	$N = q^{m-1} + \nu(u+Q(c))q^{m/2-1}$
Type II	(m odd)	$N = q^{m-1} + \tau(c,u)q^{(m-1)/2}$
Type III	(m even)	$N = q^{m-1} - \nu(u+Q(c))q^{m/2-1}$

q **odd**	
(m odd)	$N = q^{m-1} + \eta(u+R)\eta(\Delta')q^{(m-1)/2}$
(m even)	$N = q^{m-1} + \nu(u+R)\eta(\Delta')q^{m/2-1}$

Table 2.4: Number of solutions to $Q(x) + L(x) = u$

Proof. When q is even, the results for Type I and III follow from Theorem 2.3.2 after an affine change of coordinates which replaces x_1 by $x_1 + c_2$, and x_2 by $x_2 + c_1$, etc. This eliminates the linear terms and replaces u with $u + Q(c)$. In the case of Type II ($Q(x) = B_{m-1}(x) + x_m^2$), the same trick eliminates the first $m-1$ linear terms and replaces u with $u + B_{m-1}(c)$. If $c_m = 0$ then we are done: there are q^{n-1} solutions as in Theorem 2.3.2. But if $c_m \neq 0$ we are left with the equation

$$B_{m-1}(x) = x_m^2 + c_m x_m + u + B_{m-1}(c).$$

The number of solutions $(x_1, \cdots, x_{m-1})$ to this equation depends on whether or not the right side vanishes. By Theorem 2.2.15, this in turn depends on

$$t = \mathsf{Tr}_{\mathbb{F}_2}^F\left(\frac{u + B_{m-1}(c)}{c_m^2}\right).$$

If $t = 0$ then there are two values of x_m for which the right side vanishes, and $q-2$ values for which the right side is nonzero. This gives

$$N = 2\left(q^{m-2} + (q-1)q^{(m-1)/2-1}\right) + (q-2)\left(q^{m-2} - q^{(m-1)/2-1}\right) = q^{m-1} + q^{(m-1)/2}.$$

If $t \neq 0$ then the right side never vanishes, so choosing x_m arbitrarily and then choosing the other variables $x_1, \cdots, x_{m-1}$ gives

$$N = q\left(q^{m-2} - q^{(m-1)/2-1}\right) = q^{m-1} - q^{(m-1)/2}.$$

If q is odd we may assume $Q(x) = \sum_{i=1}^{m} a_i x_i^2$ with $a_i \neq 0$ for all i. The substitution $x_i \to y_i - b_i/2a_i$ converts the equation $Q(x) + L(x) = u$ into the equation $Q(y) = u + R$ where

$$R = \text{“}Q\left(\frac{c}{2a}\right)\text{”} = a_1\left(\frac{c_1}{2a_1}\right)^2 + a_2\left(\frac{c_2}{2a_2}\right)^2 + \cdots + a_m\left(\frac{c_m}{2a_m}\right)^2. \tag{2.13}$$

By Theorem 2.3.2 the number of solutions to this equation is

$$N = q^{m-1} + \begin{cases} \eta(u+R)\eta(\Delta')q^{(m-1)/2} & \text{if } m \text{ is odd} \\ \nu(u+R)\eta(\Delta')q^{m/2-1} & \text{if } m \text{ is even.} \end{cases}$$

This completes the proof of Theorem 2.3.4. □

2.3.c The Quadratic form $\mathsf{Tr}(cx^d)$ for $d = q^i + q^j$

One important source of quadratic forms is the following. Let $F = \mathbb{F}_q \subset L = \mathbb{F}_{q^n}$ be finite fields. Let $c \in L$. Let $d = 1 + q^i$. Then, as shown below, the function $Q : L \to F$ defined by

$$Q(x) = \mathsf{Tr}_F^L(cx^d) \tag{2.14}$$

is a quadratic form. We may assume that $i < n$ because $x^{q^n} = x$ for all $x \in L$. We remark that the function $\mathsf{Tr}_F^L(cx^{d'})$ where $d' = q^j + q^i$ is no more general than (2.14), because the change of variable $y = x^{q^j}$ converts this form into $\mathsf{Tr}_F^L(cx^e)$ where $e = 1 + q^{i-j}$.

Theorem 2.3.5. *If $d = 1 + q^i$ then the function $Q(x) = \mathsf{Tr}_F^L(cx^d)$ is a quadratic form over F. Let $g = \gcd(i, n)$. The rank of this quadratic form is given in Table 2.5, where $g = \gcd(n, i)$, $e = 1+q^g$, $\eta = \eta(\Delta')$ as in equation (2.9), and $c = s^d$ means that c is a d-th power of some element $s \in L$.*

The following lemma is used in the proof of Theorem 2.3.5.

Lemma 2.3.6. *Let $n, j \geq 1$ and $b \geq 2$. The greatest common divisor $g = \gcd(n, j)$ is given in Table 2.6.*

Proof. The first statement follows from a simple calculation. It is possible to use the identity $b^{2k} - 1 = (b^k - 1)(b^k + 1)$ (with $k = j$ and $k = n$ respectively) to deduce the second and third statements from the first statement. □

q **even**				
Conditions			Type	Rank
n/g even	$n/2g$ odd	$c = s^d$	I	$n - 2g$
		$c \neq s^d$	III	n
	$n/2g$ even	$c = s^d$	III	$n - 2g$
		$c \neq s^d$	I	n
n/g odd			II	$n - g + 1$

q **odd**				
Conditions			Type	Rank
n/g even	$n/2g$ odd	$c^2 = s^e$ $c \neq s^e$	$\eta = -1$	$n - 2g$
		otherwise	$\eta = 1$	n
	$n/2g$ even	$c = s^e$	$\eta = 1$	$n - 2g$
		$c \neq s^e$	$\eta = -1$	n
n/g odd	n odd			n
	n even			n

Table 2.5: The quadratic form $\mathsf{Tr}(cx^d)$, $d = 1 + q^i$

$$\gcd(b^n - 1, b^j - 1) = b^g - 1$$

$$\gcd(b^n - 1, b^j + 1) = \begin{cases} 1 + b^g & \text{if } n/g \text{ is even} \\ 2 & \text{if } n/g \text{ is odd and } b \text{ is odd} \\ 1 & \text{if } n/g \text{ is odd and } b \text{ is even} \end{cases}$$

$$\gcd(b^n + 1, b^j + 1) = \begin{cases} 1 + b^g & \text{if } n/g \text{ is odd and } j/g \text{ is odd} \\ 2 & \text{if } n/g \text{ is even or } j/g \text{ is even, and } b \text{ is odd} \\ 1 & \text{if } n/g \text{ is even or } j/g \text{ is even, and } b \text{ is even} \end{cases}$$

Table 2.6: $\gcd(b^n \pm 1, b^j \pm 1)$

Proof of Theorem 2.3.5 Let $e_1, e_2, \cdots, e_r$ be a basis for L as a vector space over F. Let

$x = a_1e_1 + \cdots + a_re_r \in L$. Then

$$\begin{aligned}
\mathsf{Tr}_F^L(cx^{1+q^i}) &= \mathsf{Tr}_F^L\left[c\left(\sum_{h=1}^r a_he_h\right)\left(\sum_{h=1}^r a_he_h\right)^{q^i}\right] \\
&= \mathsf{Tr}_F^L\left[c\left(\sum_{h=1}^r a_he_h\right)\left(\sum_{h=1}^r a_he_h^{q_i}\right)\right] \\
&= \sum_{h=1}^r\sum_{k=1}^r b_{hk}a_ha_k
\end{aligned}$$

where

$$b_{hk} = \mathsf{Tr}_F^L\left(ce_he_k^{q^i}\right).$$

This is a quadratic form. In order to determine its rank we start by determining its kernel $W = \mathrm{Ker(Q)}$. Equating

$$\mathsf{Tr}_F^L(c(y+w)^{1+q^i}) = \mathsf{Tr}_F^L(cy^{1+q^i})$$

gives

$$\mathsf{Tr}_F^L(cw^{1+q^i} + cyw^{q^i} + cy^{q^i}w) = 0.$$

Hence $w \in W$ if and only if

$$\mathsf{Tr}_F^L(cw^{1+q^i}) = 0 \tag{2.15}$$

and

$$\mathsf{Tr}_F^L(cwy^{q^i}) = -\mathsf{Tr}_F^L(cw^{q^i}y) \text{ for every } y \in L.$$

Since $\mathsf{Tr}_F^L(x^q) = \mathsf{Tr}_F^L(x)$ the right side of this equation is unchanged if we raise its argument to the power q^i, which gives

$$\mathsf{Tr}_F^L((cw + c^{q^i}w^{q^{2i}})y^{q^i}) = 0$$

for all $y \in L$, so

$$cw = -c^{q^i}w^{q^2i}$$

or, assuming $w \neq 0$,

$$c^{q^i-1}w^{q^{2i}-1} = -1. \tag{2.16}$$

Let

$$z = cw^{1+q^i}.$$

Then equation (2.16) is equivalent to:

$$z^{q^i-1} = -1. \tag{2.17}$$

At this point we must separate the cases, when q is even or odd. From here on we let $g = \gcd(n, i)$.

q **even:** Here,

$$z^{q^i-1} = -1 = 1$$

so an element $w \in L$ is in Ker(Q) if and only if:

$$z = cw^{1+q^i} \in \mathbb{F}_{q^i} \cap \mathbb{F}_{q^n} = \mathbb{F}_{q^g} \quad \text{and} \quad \mathsf{Tr}_F^L(z) = 0. \tag{2.18}$$

The set

$$\mathbb{F}_{q^g} \cap \mathrm{Ker}(\mathsf{Tr}_{\mathrm{F}}^{\mathrm{L}})$$

is either all of $\mathbb{F}_{q^g}$, which is a vector space of dimension g, or it is a hyperplane in $\mathbb{F}_{q^g}$, which therefore has dimension $g-1$. It remains to determine the number of elements $w \in L$ that satisfy equation (2.17) with

$$z \in \mathbb{F}_{q^g} \cap \mathrm{Ker}(\mathsf{Tr}_{\mathrm{F}}^{\mathrm{L}}).$$

We claim that $W = \mathrm{Ker}(\mathrm{Q})$ is nonzero if and only if there exists $s \in L$ so that $s^d = c$. That is, so that

$$s^{1+q^i} = c. \tag{2.19}$$

First, suppose such an s exists. Then every element

$$z' \in \mathbb{F}_{q^g} \cap \mathrm{Ker}\left(\mathsf{Tr}_{\mathrm{K}}^{\mathrm{L}}\right)$$

gives rise to an element $w' \in \mathrm{Ker}(\mathrm{Q})$ as follows. Since $1+q^i$ is relatively prime to q^i-1 and hence also to q^g-1 there exists $h' \in \mathbb{F}_{q^g}$ such that

$$(h')^{1+q^i} = z'.$$

Set $w' = h'/s \in L$. It follows that

$$z' = c(w')^{1+q^i}$$

so w' satisfies equations (2.15) and (2.16).

We remark that if n/g is odd then $1+q^i$ is relatively prime to q^n-1 so such an element s satisfying equation (2.19) exists, hence the dimension of $W = \mathrm{Ker}(\mathrm{Q})$ is $g-1$. If n/g is even and if such an element s exists, then

$$\mathbb{F}_{q^g} \cap \mathrm{Ker}(\mathsf{Tr}_{\mathrm{K}}^{\mathrm{L}}) = \mathbb{F}_{\mathrm{q^g}};$$

for if $z' \in \mathbb{F}_{q^g}$ and n/g is even then (writing $E = \mathbb{F}_{q^g}$ to ease notation),

$$\mathsf{Tr}_F^L(z') = \mathsf{Tr}_F^E \mathsf{Tr}_E^L(z') = (n/g)\mathsf{Tr}_F^E(z') = 0. \tag{2.20}$$

Thus, in this case, the dimension of $W = \mathrm{Ker}(\mathrm{Q})$ is g.

Next, we prove the converse: suppose there exists $w \neq 0 \in W$; we claim there exists $s \in L$ satisfying equation (2.19). We may suppose that n/g is even (since the odd case was handled above). We find an element $u \neq 0 \in L$ so that u^{q^i+1} is a primitive element of $\mathbb{F}_{q^g}$. This will suffice because $z = cw^{q^i+1} \in \mathbb{F}_{q^g}$ so there exists m with $z = u^{(q^i+1)m}$, hence $c = (u^m/w)^{q^i+1}$.

The element $u \in L = \mathbb{F}_{q^n}$ should be taken to be a primitive element of the sub-field $\mathbb{F}_{q^{2g}}$ (which is contained in L since n/g is even). Then

$$u^{q^{2g}-1} = u^{(q^g-1)(q^g+1)} = 1.$$

Moreover, $u^{q^i+1} \in \mathbb{F}_{q^g}$ for the following reason: i/g is odd so by Lemma 2.3.6, q^g+1 divides q^i+1. Therefore

$$u^{(q^g-1)(q^i+1)} = 1.$$

Finally, u^{q^i+1} is primitive in $\mathbb{F}_{q^g}$ because q^i+1 and q^g-1 are relatively prime. We remark that as u varies within the field $\mathbb{F}_{q^{2g}}$ the element uw varies within Ker(Q) because

$$c(uw)^{1+q^i} \in \mathbb{F}_{q^i} \cap \mathbb{F}_{q^n}$$

and the trace condition is satisfied by equation (2.20). So in this case, $\dim(\mathrm{Ker}(\mathrm{Q})) = 2\mathrm{g}$.

q odd: In this case

$$z^{q^i-1} = -1$$

so $z^2 \in \mathbb{F}_{q^i}$. Hence

$$z \in \mathbb{F}_{q^{2i}} \cap \mathbb{F}_{q^n} = \mathbb{F}_{q^{\gcd(n,2i)}}.$$

If n/g is odd then $\gcd(n, 2i) = \gcd(n, i) = g$, so $z \in \mathbb{F}_{q^g} \subset \mathbb{F}_{q^i}$. Hence

$$z^{q^i-1} = 1, \tag{2.21}$$

which is a contradiction. Therefore $w = 0$, so the quadratic form Q has maximal rank, n.

Now suppose n/g is even, so $\gcd(n, 2i) = 2g$. Equation (2.21) holds, so

$$z^2 \in \mathbb{F}_{q^i} \cap \mathbb{F}_{q^n} = \mathbb{F}_{q^g},$$

so

$$z^{q^g-1} = \pm 1.$$

The $+1$ is not possible, so

$$z^{q^g-1} = -1. \tag{2.22}$$

We claim that

$$\text{if } x \in L = \mathbb{F}_{q^n} \text{ and } x^{q^g-1} = -1 \text{ then } \mathsf{Tr}_F^L(x) = 0.$$

For $x^{q^g} = -x$, let $T = x + x^q + \cdots + x^{q^{g-1}}$. Then

$$\mathsf{Tr}_F^L(x) = \mathsf{Tr}_F^E \mathsf{Tr}_E^L(x) = T - T + T - T \cdots \pm T$$

(where $E = \mathbb{F}_{q^g}$) and there are n/g terms (an even number), so this last sum vanishes.

It follows that (when n/g is even), $w \in \mathrm{Ker(Q)}$ if and only if

$$z = cw^{1+q^i}$$

satisfies equation (2.22). Thus, if $a \in \mathbb{F}_{q^{2g}}$ and $w \in \mathrm{Ker(Q)}$ then $aw \in \mathrm{Ker(Q)}$. If $v, w \neq 0 \in \mathrm{Ker(Q)}$ then

$$(v/w)^{(1+q^i)(q^i-1)} = 1$$

so

$$v/w \in \mathbb{F}_{q^{2i}} \cap \mathbb{F}_{q^n} = \mathbb{F}_{q^{2g}}.$$

In summary, either $\mathrm{Ker(Q)} = \{0\}$ or $\mathrm{Ker(Q)}$ has dimension $2g$.

It remains to determine when $\mathrm{Ker(Q)}$ has a nonzero element. Let $\alpha \in \mathbb{F}_{q^n}$ be a primitive element and set $c = \alpha^\ell$. Equation (2.22) becomes

$$\alpha^\ell w^{(1+q^i)} = \alpha^{(q^n-1)/2(q^g-1)}.$$

So we search for $w = \alpha^r$ such that $\alpha^{\ell + r(1+q^i)} = \alpha^{(q^n-1)/2(q^g-1)}$ or

$$\ell \equiv \frac{q^n - 1}{2(q^g - 1)} \pmod{q^g + 1}$$

since $\gcd(q^i + 1, q^n - 1) = q^g + 1$ in this case. If $n/(2g)$ is even then $q^g + 1$ divides $(q^n - 1)/2(q^g - 1)$ hence $w \neq 0$ exists if and only if $\ell \equiv 0 \pmod{q^g + 1}$, which is to say that $c = s^e$ for some $s \in L$, where $e = q^g + 1$. If $n/(2g)$ is odd then

$$\frac{q^n - 1}{2(q^g - 1)} \equiv \frac{q^g + 1}{2} \pmod{q^g + 1}$$

so $w \neq 0$ exists if and only if $\ell \equiv (q^g + 1)/2 \pmod{q^g + 1}$.

Determining $\eta(\Delta')$ We do not know $\eta(\Delta')$ when q is odd and n/g is odd. But if q is odd and n/g is even, it is possible to determine when $\Delta'(Q)$ is a square because this is detected (according to Theorem 2.3.2) by the number $|Z|$ of nonzero solutions Z to the equation $Q(x) = 0$. If $x \in Z$ and $0 \neq a \in L$ and if $a^{1+q^i} \in F$ then $a^{1+q^i} x \in Z$. Hence the group

$$G = \{a \in L : \ a^{1+q^i} \in F\} = \{a \in L : \ a^{(1+q^i)(q-1)} = 1\}$$

acts freely on Z so $|G| = (1+q^g)(q-1)$ divides $|Z|$. If n/g is even this says,

$$\frac{|G|}{q-1} = (q^g+1) \text{ divides } \frac{|Z|}{q-1} = \frac{q^n-1}{q-1} - \frac{q^{n-1}}{q^{\mathrm{rank}(Q)/2}}\left(q^{\mathrm{rank}(Q)/2} - \eta(\Delta'(Q))\right)$$

with $\eta(\Delta'(Q)) = \pm 1$. Together with the rank of Q determined above and the divisibility properties in Lemma 2.3.6, this gives the values of $\eta(\Delta'(Q))$ listed in Theorem 2.3.5. □

Corollary 2.3.7. *Let $F = \mathbb{F}_q \subset L = \mathbb{F}_{q^n}$ be finite fields, let $d = 1+q^i$, let $A, B \in L$ with $B \neq 0$, and let $F : L \to F$ be the function*

$$F(x) = \mathsf{Tr}_F^L(Ax + Bx^d).$$

Then F is identically zero if and only if the following conditions hold.

1. *$A = 0$.*
2. *n is even and $\gcd(i,n) = n/2$.*
3. *$\mathsf{Tr}_E^L(B) = 0$ where $E = \mathbb{F}_{q^{n/2}}$ (so that $F \subset E \subset L$.)*

Proof. We may assume that $i < n$ (since $x^{q^n} = x$ for all $x \in L$), so the second condition is equivalent to $i = n/2$. If the three conditions hold then $d = (|L|-1)/(|E|-1)$ so $x^d \in E$ for any $x \in L$. Therefore

$$\mathsf{Tr}_F^E\left(\mathsf{Tr}_E^L(Bx^d)\right) = \mathsf{Tr}_F^E\left(x^d \mathsf{Tr}_E^L(B)\right) = 0.$$

To prove the converse, let $L(x) = \mathsf{Tr}_F^L(Ax)$ and $Q(x) = \mathsf{Tr}_F^L(Bx^d)$. Suppose $F(x) = L(x) + Q(x)$ is identically zero. If $A \neq 0$ then Proposition 2.3.3 implies that Ker(Q) $\subset$ Ker(L) so Q is a non-vanishing quadratic form of some rank $m > 0$. So there exists a subspace $V \subset E$ whose F-dimension is m, such that the restriction of Q to V is non-degenerate. But $N_0 = q^n$ since F is identically zero, so in the notation of Proposition 2.3.3, $N_0' = q^m$, which is to say that the restriction of Q to V is zero. This is a contradiction. Therefore $A = 0$ which proves (1). Therefore the quadratic form Q has rank zero. By theorem 2.3.5 (and Table 2.5) it follows that $n = 2g$ where $g = \gcd(i,n)$, which proves (2). Thus $g = i = n/2$. To prove (3) we must consider two cases, depending on the parity of q. Let $E = \mathbb{F}_{q^g}$.

First suppose q is even. From Table 2.5 we see that $B = s^d$ for some $s \in E$. Therefore

$$\mathsf{Tr}_E^L(B) = s^d + s^{dq^g} = s^{1+q^g} + s^{(1+q^g)q^g} = s^{1+q^g} + s^{q^g+1} = 0.$$

Now suppose q is odd. From Table 2.5 we see (since $n/2g = 1$ is odd) that

$$B^2 = s^{1+q^g}$$

(for some $s \in L$) but B cannot be so expressed. Therefore

$$B^{q^g-1} = -1$$

since its square is

$$s^{(1+q^g)(q^g-1)} = 1.$$

In summary,

$$\mathsf{Tr}_E^L(B) = B + B^{q^g-1+1} = B - B = 0. \qquad \square$$

2.4 Algebraic number fields

2.4.a Basic properties

So far our examples of fields have consisted of finite fields and the familiar fields $\mathbb{Q}$, the rational numbers, $\mathbb{R}$, the real numbers, and $\mathbb{C}$, the complex numbers. Recall that we we obtain the various finite fields of characteristic $p > 0$ from the prime field $\mathbb{F}_p$ by constructing the quotient $\mathbb{F}_p[x]/(f(x))$ where $f(x)$ is an irreducible polynomial. We can think of this construction as adjoining a root (the variable x) of $f(x)$ to the field $\mathbb{F}_p$. Similarly, we obtain the complex numbers from the real numbers by adjoining a root of the polynomial $x^2 + 1$.

In this section we study a class of fields, called *algebraic number fields* that are obtained in the same way from the rational numbers. For the most part we omit proofs and leave the interested reader to find them in other references.

Definition 2.4.1. *An algebraic number field E is a finite extension of the rational numbers $\mathbb{Q}$.*

This means that E is a field that contains $\mathbb{Q}$ and that as a vector space over $\mathbb{Q}$ it is finite dimensional.

A complex number $a \in \mathbb{C}$ is *algebraic over* $\mathbb{Q}$, or simply *algebraic*, if it is a root of some polynomial $f(x) \in \mathbb{Q}[x]$ with coefficients in $\mathbb{Q}$. As in Theorem 1.4.11, there exists a unique monic minimal polynomial $f(x) \in \mathbb{Q}[x]$, irreducible in $\mathbb{Q}[x]$, such that $f(a) = 0$. If $\mathbb{Q}(a) \subset \mathbb{C}$ denotes the smallest field that contains both $\mathbb{Q}$ and a, then the mapping $\mathbb{Q}[x] \to \mathbb{Q}(a)$ which takes x to a induces an isomorphism

$$\mathbb{Q}[x]/(f) \to \mathbb{Q}(a),$$

where f is the minimal polynomial of a. The proof is left as an exercise. An important result is the following:

Theorem 2.4.2. *Suppose that E and F are algebraic number fields with $F \subseteq E$. Then there is an element $a \in E$ such that $E = F(a)$. In particular, every algebraic number field is of the form $\mathbb{Q}(a)$ for some algebraic number a.*

A field F is *algebraically closed* if every polynomial with coefficients in F splits as a product of linear factors. Every field is contained in an algebraically closed field, and any two minimal algebraically closed fields containing a given field F are isomorphic. Thus in general we may speak of *the* algebraic closure of a field F.

For example, $\mathbb{C}$ is algebraically closed. The set $\overline{\mathbb{Q}}$ of all algebraic numbers over $\mathbb{Q}$ is an algebraically closed subfield of $\mathbb{C}$, and we shall refer to this particular field as the algebraic closure of $\mathbb{Q}$. It is not a finite extension of $\mathbb{Q}$, so it is not a number field. However, this observation allows us to embed any algebraic number field in the complex numbers. For any prime number p, the set

$$\mathbb{F}_{p^\infty} = \cup_d \mathbb{F}_{p^d}$$

is a field. It is the algebraic closure of every $\mathbb{F}_{p^d}$.

Theorem 2.4.3. *Let F be a number field. Then there are exactly $[F:\mathbb{Q}]$ embeddings of F in $\mathbb{C}$. If $K \subset F$ is a subfield then every embedding $\tau : K \to \mathbb{C}$ extends to $[F:K]$ distinct embeddings $\sigma : F \to \mathbb{C}$ such that $\sigma(b) = \tau(b)$ for all $b \in K$.*

Proof. Let $F = \mathbb{Q}(a)$. An embedding σ of F in $\mathbb{C}$ is completely determined by its value on a. The image $\sigma(a)$ is a root of the minimal polynomial $f \in \mathbb{Q}[x]$ of a over $\mathbb{Q}$ (thinking of f as a polynomial over $\mathbb{C}$). It is straightforward to check that every root of f determines an embedding. The number of roots of f is exactly its degree, since $\mathbb{C}$ is algebraically closed. Thus the number of embeddings of F in $\mathbb{C}$ is exactly the degree of f, which equals $[F:\mathbb{Q}]$. The proof of the second statement is similar, and is left as an exercise. □

Theorem 2.4.4. *Let F be a number field and let $\sigma_1, \cdots, \sigma_d$ be the distinct embeddings of F in $\mathbb{C}$. Let $b \in F$ and let $e = [\mathbb{Q}(b):\mathbb{Q}]$. Then*

1. $\mathsf{Tr}_{\mathbb{Q}}^{F}(b) = \sigma_1(b) + \sigma_2(b) + \cdots + \sigma_d(b) = e\mathsf{Tr}_{\mathbb{Q}}^{\mathbb{Q}(b)}(b)$.
2. $\mathsf{N}_{\mathbb{Q}}^{F}(b) = \sigma_1(b)\sigma_2(b)\cdots\sigma_d(b) = \left(\mathsf{N}_{\mathbb{Q}}^{\mathbb{Q}(b)}(b)\right)^e$.
3. *If F is a Galois extension of $\mathbb{Q}$ then*

$$\mathsf{Tr}_{\mathbb{Q}}^{F}(b) = \sum_{\sigma \in \mathrm{Gal}(F/\mathbb{Q})} \sigma(b) \quad \text{and} \quad \mathsf{N}_{\mathbb{Q}}^{F}(b) = \prod_{\sigma \in \mathrm{Gal}(F/\mathbb{Q})} \sigma(b).$$

4. *The trace map $\mathsf{Tr}_{\mathbb{Q}}^{F} : F \to \mathbb{Q}$ is surjective.*

Proof. (See also Theorem 2.2.14.) Let $f(x) = a_0 + a_1 x + \cdots + a_e x^e$ be the minimum polynomial of b. By definition, the roots of f (in $\mathbb{C}$) are distinct (although they are not necessarily all contained in $\mathbb{Q}(b)$ or even in F). The set $\{1, b, b^2, \cdots, b^{e-1}\}$ forms a basis for $\mathbb{Q}(b)$ as a vector space over $\mathbb{Q}$. With respect to this basis, the matrix M_b for the mapping $\ell_b : \mathbb{Q}(b) \to \mathbb{Q}(b)$ ($\ell_b(a) = ba$) is the

companion matrix of $f(x)$,that is, it has ones on the superdiagonal, $-a_0, -a_1, \cdots, -a_{e-1}$ in the last rown, and zeroes elsewhere. See equation (2.3). The characteristic polynomial of M_b is exactly the polynomial $f(x)$ and the eigenvalues of M_b are the distinct roots of $f(x)$. So the trace and norm of b are the sum and product of the roots of $f(x)$ which are

$$\mathsf{Tr}_{\mathbb{Q}}^{\mathbb{Q}(b)}(b) = -a_{e-1} \quad \text{and} \quad \mathsf{N}_{\mathbb{Q}}^{\mathbb{Q}(b)}(b) = (-1)^e a_e.$$

Let $\tau_1, \cdots, \tau_e$ denote the distinct embeddings of $\mathbb{Q}(b)$ into $\mathbb{C}$. The elements $\tau_1(b), \tau_2(b), \cdots, \tau_e(b)$ are exactly the roots of the polynomial f. Consequently

$$\mathsf{Tr}_{\mathbb{Q}}^{\mathbb{Q}(b)}(b) = \tau_1(b) + \cdots + \tau_e(b) \quad \text{and } \mathsf{N}_{\mathbb{Q}}^{\mathbb{Q}(b)}(b) = \tau_1(b)\tau_2(b)\cdots\tau_e(b).$$

Let $u_1, \cdots, u_t$ be a basis for F over $\mathbb{Q}(b)$ (hence $te = d$). Then the set $\{u_i b^j\}$ $(1 \le i \le t,$ $0 \le j \le e-1)$ forms a basis for F over $\mathbb{Q}$. With respect to this basis the mapping $L_b : F \to F$ $(L_b(a) = ba)$ is a "block matrix" with t diagonal blocks, each of which is a copy of the matrix M_b. It follows that the characteristic polynomial of L_b is $(f(x))^t$, that $\mathsf{Tr}(L_b) = t\mathsf{Tr}(M_b)$ and that $\det(L_b) = (\det(M_b))^t$. By Theorem 2.4.3, each embedding $\tau_i : \mathbb{Q}(b) \to \mathbb{C}$ extends to t distinct embeddings $F \to \mathbb{C}$ but these embeddings all take $b \in F$ to the same element, $\tau_i(b)$. Therefore

$$\sum_{i=1}^{d} \sigma_i(b) = t \sum_{i=1}^{e} \tau_i(b) = t\mathsf{Tr}(M_b) = \mathsf{Tr}(L_b) = \mathsf{Tr}_{\mathbb{Q}}^{F}(b)$$

and

$$\prod_{i=1}^{d} \sigma_i(b) = \prod_{i=1}^{e} \tau_i(b)^t = (\det(M_b))^t = \det(L_b) = \mathsf{N}_{\mathbb{Q}}^{F}(b).$$

If F is a Galois extension of $\mathbb{Q}$ then the embeddings $\sigma_i : F \to \mathbb{C}$ have the same image, and the Galois group $\mathrm{Gal}(F/Q)$ permutes these embeddings. Consequently,

$$\mathsf{Tr}_{\mathbb{Q}}^{F}(b) = \sum_{\sigma \in \mathrm{Gal}(F/\mathbb{Q})} \sigma(b) \quad \text{and} \quad \mathsf{N}_{\mathbb{Q}}^{F}(b) = \prod_{\sigma \in \mathrm{Gal}(F/\mathbb{Q})} \sigma(b).$$

Finally, the trace $\mathsf{Tr}_{\mathbb{Q}}^{F}$ is surjective if and only if it is nonzero, but $\mathsf{Tr}_{\mathbb{Q}}^{F}(1) = d \neq 0$. □

2.4.b Algebraic integers

Just as algebraic number fields are generalizations of the rational numbers, there is a generalization of the rational integers $\mathbb{Z}$.

Definition 2.4.5. *An algebraic number a is an* algebraic integer *or is* integral *if its minimal polynomial $f \in \mathbb{Q}[x]$ over $\mathbb{Q}$ has all its coefficients in $\mathbb{Z}$.*

Theorem 2.4.6. *The following are equivalent*

1. *a is an algebraic integer.*
2. *$\mathbb{Z}[a]$ is a finitely generated $\mathbb{Z}$-module.*
3. *$a \in R$ for some ring $R \subseteq \mathbb{C}$ that is a finitely generated $\mathbb{Z}$-module.*
4. *$aM \subseteq M$ for some finitely generated $\mathbb{Z}$-module $M \subseteq \mathbb{C}$.*

Proof. If a is an algebraic integer, then a^d is a linear combination of $1, a, \cdots, a^{d-1}$ with integer coefficients, and it follows that $\mathbb{Z}[a]$ is generated as a $\mathbb{Z}$-module by $1, a, \cdots, a^{d-1}$. The implications (2) $\Longrightarrow$ (3) $\Longrightarrow$ (4) are straightforward.

To prove that (4) implies (1), suppose that M is generated by $m_1, \cdots, m_k$. Thus for $j = 1, \cdots, k$, we have

$$am_j = \sum_{i=1}^{k} b_{i,j} m_j \tag{2.23}$$

with $b_{i,j} \in \mathbb{Z}$. Let $c_{i,j} = b_{i,j}$ if $i \neq j$, and $c_{i,i} = b_{i,i} - x$. It follows from equation (2.23) that the determinant of the matrix $[c_{ij}]$ is zero at $x = a$. But the determinant of this matrix is a monic polynomial with integer coefficients, so a is algebraic. □

2.4.c Orders

Let F be an algebraic number field and let $m = [F : \mathbb{Q}]$. If $R \subset F$ is a subring, then it is automatically an integral domain. An *order* $R \subset F$ is a subring of F that is finitely generated as a $\mathbb{Z}$-module with rank m. In this case, Corollary 1.1.18 implies that R^+ is isomorphic to $\mathbb{Z}^m$. A standard result is the following.

Theorem 2.4.7. *A subring R in a number field F is an order in F if and only if it satisfies the following three conditions,*

1. *$R \cap \mathbb{Q} = \mathbb{Z}$*
2. *The fraction field (Section 1.2.h) of R is F.*
3. *The Abelian group $(R, +)$ is finitely generated.*

Except when $F = \mathbb{Q}$, there are infinitely many orders in F. Every order $R \subset F$ consists entirely of algebraic integers and in fact the intersection $\mathbb{Z}_F = F \cap \mathbb{F}A$ (where $\mathbb{F}A$ denotes the set of all algebraic integers) is an order which contains all the other orders in F. This maximal order $\mathbb{Z}_F$ is called the *ring of integers* of F. It is *integrally closed* in F, meaning that if $\alpha \in F$ is a root of a *monic* polynomial with coefficients in $\mathbb{Z}_F$ then $\alpha \in \mathbb{Z}_F$ also. In fact, $\mathbb{Z}_F$ is the integral closure of $\mathbb{Z}$ in F, that is, it consists of all elements $\alpha \in F$ which are roots of monic polynomials with coefficients in $\mathbb{Z}$. So a subset $R \subset F$ is an order if and only if it is a subring and it is contained in $\mathbb{Z}_F$ as a subgroup of finite index.

The ring of integers of $\mathbb{Q}$ is $\mathbb{Z}$; the ring of integers of $\mathbb{Q}[i]$ is $\mathbb{Z}[i]$. However the ring of integers of $\mathbb{Q}[\sqrt{5}]$ is larger than $\mathbb{Z}[\sqrt{5}]$ (which is an order). Rather, the ring of integers consists of all integer linear combinations of $(1+\sqrt{5})/2$ and $(1-\sqrt{5})/2$. For any number field F the maximal order $\mathbb{Z}_F$ has several particularly nice properties (it is a Dedekind ring, for example).

Lemma 2.4.8. *Let R be an order in a number field F. Let $a \in R$. Then the number of elements in the quotient ring is $|R/(a)| = |\mathsf{N}(a)|$.*

Proof. (See also Exercise 5.) Let $\{u_1, \cdots, u_n\}$ be an integer basis for the $\mathbb{Z}$-module R. Then the set $\{au_1, \cdots, au_n\}$ is an integer basis for the $\mathbb{Z}$-module (a). Each au_i is some integer linear combination, say, $au_i = A_{i1}u_1 + \cdots + A_{in}u_n$. On the one hand, the matrix $A = (A_{ij})$ describes the action of multiplication by a on M so $\mathsf{N}(a) = \det(A)$. On the other hand, according to Theorem 1.2.28, $|R/(a)| = |\det(A)|$. □

In particular, the theorem says that the norm of any algebraic integer is an ordinary integer. The absolute value of the norm gives a candidate function for defining division with remainder, see Definition 1.2.13. If $F = \mathbb{Q}(\sqrt{d})$ is a quadratic number field then its ring of integers is a Euclidean domain with respect to this function if and only if d =2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73, -1, -2, -3, -7, -11, see [3] Section 3.2. A number field has *class number* one if and only if its ring of integers is a unique factorization domain. The *Stark-Heegner Theorem* states that the only quadratic imaginary number fields with class number one are $\mathbb{Q}(\sqrt{d})$ for $d = -1$, -2, -3, -7, -11, -19, -43, -67, -163. However the ring of integers of any number field is a *Dedekind domain*, and as such it admits unique prime decomposition of ideals, i.e., for any ideal I there are uniquely determined prime ideals $P_1, P_2, \cdots, P_k$ and integers $m_1, m_2, \cdots, m_k$ so that $I = P_1^{m_1} P_2^{m_2} \cdots P_k^{m_k}$. Moreover, we next show that every element in an order can be written in at least one way as a product of irreducible elements, so it is a *factorization ring*.

Theorem 2.4.9. *Let R be an order in a number field F and let $a \in R$. Then there is a unit u and irreducible elements $f_1, \cdots, f_k \in R$ so that $a = uf_1f_2 \cdots f_k$. (If a is not a unit then the element u can be absorbed into one of the irreducible factors.)*

Proof. Use induction on $|\mathsf{N}(a)|$. If $|\mathsf{N}(a)| = 1$, then a is a unit so we are done. Likewise, if a is irreducible we are done. Otherwise we can write $a = bc$ where neither b nor c is a unit. Then $|\mathsf{N}(a)| = |\mathsf{N}(b)||\mathsf{N}(c)|$ and neither $|\mathsf{N}(b)|$ nor $|\mathsf{N}(c)|$ is equal to 1. Thus $|\mathsf{N}(b)| < |\mathsf{N}(a)|$ and $|\mathsf{N}(c)| < |\mathsf{N}(a)|$. By induction both b and c can be written as units times a product of irreducible elements, and we can combine these expressions into such an expression for a. □

2.5 Local and global fields

2.5.a Local fields

There are two types of *local fields*: local function fields, and p-adic fields. They are discussed in more detail in Section 4.6.c (where local fields are defined) but here are the basic definitions. If F is a field, then the (local) *function field* $F((x))$ consists of all *formal Laurent series* $\sum_{i=-k}^{\infty} a_i x^i$, with $a_i \in F$. Such a series has finitely many terms of negative degree and possibly infinitely many terms of positive degree. Its ring of "integers" is the subring $F[[x]]$ of formal power series, that is, sums with no terms of negative degree. The ring $F[[x]]$ is a local ring with unique maximal ideal (x). The field $F((x))$ is the fraction field of $F[[x]]$. That is, every formal Laurent series $a(x) \in F((x))$ may be expressed as a quotient $a(x) = f(x)/g(x)$ of two formal power series $f, g \in F[[x]]$ (and in fact the denominator $g(x)$ may be chosen to be a power of x). Addition and multiplication in $F((x))$ are performed in a way that is analogous to the addition and multiplication of polynomials. One must check that only finitely many terms contribute to any term in a product.

Let p be a prime number. The p-adic field $\mathbb{Q}_p$ consists of all formal Laurent series $\sum_{i=-k}^{\infty} a_i p^i$ (with finitely many terms of negative degree and possibly infinitely many terms of positive degree), where $0 \leq a_i \leq p-1$, and where addition and multiplication are performed "with carry". It contains a ring $\mathbb{Z}_p$ of "integers" consisting of formal power series with no terms of negative degree, which is a local ring with maximal ideal (p). The field $\mathbb{Q}_p$ is the fraction field of $\mathbb{Z}_p$: every $a \in \mathbb{Q}_p$ can be expressed as a fraction f/g with $f, g \in \mathbb{Z}_p$ and in fact the denominator g may be chosen to be a power of p. A *p-adic field* is a finite degree extension of $\mathbb{Q}_p$.

2.5.b Global fields

There are also two types of *global fields*: function fields and algebraic number fields. The algebraic number fields (= finite degree extensions of $\mathbb{Q}$) have been previously discussed in Section 2.4. Let F be a field. A *global function field* over F is any finite degree extension of the field $F(x)$ of rational functions. The field $F(x)$ is the fraction field of the ring $F[x]$ of polynomials, that is, every element of $F(x)$ is of the form f/g where f and g are polynomials. If K is a finite degree extension of $F(x)$ then there exists n so that $K \cong F[x_1, x_2, \cdots, x_n]/I$ where I is an appropriate maximal ideal in the ring $F[x_1, x_2, \cdots, x_n]$ of polynomials in n variables. One normally assumes that K has transcendance degree one over F, in other words, the set

$$V(I) = \{(x_1, x_2, \cdots, x_n) \in F^n : \ h(x) = 0 \text{ for all } h \in I\}$$

is a one dimensional algebraic variety, or an *algebraic curve*. Then K is called the field of rational functions on the algebraic curve $V(I)$.

2.6 Exercises

1. Lemma 2.2.14: Let d and e be positive integers with d dividing e. Prove that if $a \in \mathbb{F}_{p^e}$, then $a + a^{p^d} + a^{p^{2d}} + \cdots + a^{p^{e-d}} \in \mathbb{F}_{p^a}$.

2. Suppose p is prime and c, d, and e are integers with $c|d|e$. Prove that $\mathsf{Tr}_{p^c}^{p^d} \circ \mathsf{Tr}_{p^d}^{p^e} = \mathsf{Tr}_{p^c}^{p^e}$.

3. Develop an alternate definition of the trace function for a finite field F in terms of embeddings of F in its algebraic closure. Prove that your definition agrees with the previous one.

4. Let $F = \mathbb{Q}[\sqrt{5}]$. Show that the full ring of integers of F is $K = \mathbb{Z}[(1 \pm \sqrt{5})/2]$ and that the norm of an element $a + b\sqrt{5}$ is $a^2 + 5b^2$.

5. (*continued*) Let $L = \mathbb{Z}[\sqrt{5}]$. It is an order in K. Let $a = 2 \in L$. The inclusion $L \subset K$ induces a homomorphism of quotient rings $L/aL \to K/aK$. According to Lemma 2.4.8, both rings have 4 elements. Show that $L/aL \cong \mathbb{F}_2[x]/(x^2)$, that $K/aK \cong \mathbb{F}_4$, and that the mapping $L/aL \to K/KaK$ is neither injective nor surjective. (*Hint:* The elements of L/aL are represented by 0, 1, $\sqrt{5}$, $1 + \sqrt{5}$, from which multiplication and addition tables can be constructed. The ring K/aK can be similarly analyzed.)

Chapter 3 Finite Local Rings and Galois Rings

Local rings have a single maximal ideal. In algebraic geometry they are used to understand the local geometry at a single point on an algebraic variety. These rings, and especially the special case of Galois rings (see Section 3.5), generalize finite fields. They have recently been used in several constructions of error correcting codes and families of sequences with interesting correlation properties. They are useful models of multiphase signals.

3.1 Finite local rings

In this section we examine the structure of a commutative ring (with identity) which has finitely many elements. The standard reference for this section is [24]. During the last decade a considerable amount of effort has been directed towards developing linear feedback shift register sequences based on a finite local ring R. The analysis of these sequences depends on an understanding of the units in R.

Let R be a commutative ring. Recall from Definition 1.2.13 that R is a *local ring* if it contains a unique maximal ideal $\mathfrak{m}$. In this case (see Section 1.2.a), the maximal ideal $\mathfrak{m}$ consists precisely of the non-units of R. The quotient $F = R/\mathfrak{m}$ is a field and is called the *residue field* of R. For each $i \geq 0$ the quotient $\mathfrak{m}^{i-1}/\mathfrak{m}^i$ is naturally a vector space over F, because R acts on this quotient by multiplication, and $\mathfrak{m}$ acts trivially. The following are examples of finite local rings.

- any finite (Galois) field.
- $\mathbb{Z}/(p^n)$ for any prime number p, with maximal ideal (p) and residue field $\mathbb{Z}/(p)$.
- $\mathbb{F}[x]/(f^n)$, where $\mathbb{F}$ is a finite field and f is an irreducible polynomial, with maximal ideal (f) and residue field $\mathbb{F}[x]/(f)$.
- $R[x]/(f^n)$ where R is a finite local ring and f is a basic irreducible polynomial (see below).

Any commutative finite ring may be expressed as a direct sum of finite local rings. For the remainder of this section we assume that R is a finite local ring.

Basic irreducible polynomials: Let R be a finite local ring with maximal ideal $\mathfrak{m}$. Let $\mu : R \to F = R/\mathfrak{m}$ be the projection. Applying μ to each coefficient of a polynomial gives a mapping which we also denote by $\mu : R[x] \to F[x]$. A polynomial $f(x) \in R[x]$ is *regular* if it is not a zero divisor, which holds if and only if $\mu(f) \neq 0$. Let $f(x) \in R[x]$. If $\mu(f)$ is nonzero and is irreducible in $F[x]$ then f is irreducible in $R[x]$, and we refer to f as a *basic irreducible polynomial*. In this case $R[x]/(f^n)$ is again a local ring for any $n > 0$ (see ([24], XIV.10). Its maximal ideal is $\mathfrak{m}[x] + (f)$

and its residue field is $F[x]/(\mu(f))$, where $\mathfrak{m}[x]$ is the collection of those polynomials $f \in R[x]$ all of whose coefficients are in $\mathfrak{m}$.

If the leading term of a basic irreducible polynomial $f(x) \in R[x]$ is in the maximal ideal $\mathfrak{m}$ then the degree of the reduction $\mu(f) \in F[x]$ will be less than $\deg(f)$. If $f(x)$ is a *monic* polynomial then $\deg(f) = \deg(\mu(f))$ since the leading term is 1. For this reason we will often consider monic basic irreducible polynomials.

Lemma 3.1.1. *Let $f \in R[x]$ be a regular polynomial and suppose $\bar{\alpha} \in F$ is a simple zero of $\mu(f) \in F[x]$. Then f has one and only one root $\alpha \in R$ such that $\mu(\alpha) = \bar{\alpha}$.*

Proof. This is proven in Lemma (XV.1) of [24]. □

Further properties of polynomials over R are described in Section 3.3. The following is a powerful tool for studying local rings.

Theorem 3.1.2. *(Nakayama's Lemma for local rings [24], [23, p. 11]) Let R be a finite local ring with maximal ideal $\mathfrak{m}$. Let M be a module over R.*

1. *If M is finite and $\mathfrak{m}M = M$, then $M = 0$.*
2. *If N is a submodule of M and $M = N + \mathfrak{m}M$, then $N = M$.*

3.1.a Units in a finite local ring

Let R be a finite local ring with maximal ideal $\mathfrak{m}$ and residue field F. Let $R^\times$ be the set of invertible elements in R. Let $1 + \mathfrak{m} = \{1 + a : \ a \in \mathfrak{m}\}$. By [24], Theorem (V.1) and Proposition (IV.7),

- the ideal $\mathfrak{m}$ consists precisely of the non-units of R,
- for every $a \in R$, at least one of a and $1 + a$ is a unit, and
- there is a positive integer n such that $\mathfrak{m}^n = 0$.

The details are left as an exercise.

An element a is *nilpotent* if for some natural number k we have $a^k = 0$. It follows from the above that every element a of R is either a unit or is nilpotent. In fact we can take the same k for all a.

Proposition 3.1.3. *There exists an isomorphism of Abelian groups*

$$R^\times \cong F^\times \times (1 + \mathfrak{m}) \tag{3.1}$$

Proof. Let n be the smallest integer such that $\mathfrak{m}^n = 0$. It is called the *degree of nilpotency* of $\mathfrak{m}$. As in [24] Exercise (V.9), we have a sequence of surjective ring homomorphisms

$$R = R/\mathfrak{m}^n \xrightarrow{\sigma_n} R/\mathfrak{m}^{n-1} \xrightarrow{\sigma_{n-1}} \cdots \xrightarrow{\sigma_2} R/\mathfrak{m} = F.$$

For $2 \leq i \leq n$, the kernel $\mathrm{Ker}(\sigma_i) = \mathfrak{m}^{i-1}/\mathfrak{m}^i$ is a vector space over F. If $|F| = q$ it follows by induction that there exists an integer j such that

$$|\mathfrak{m}| = q^j \quad \text{and} \quad |R| = q^{j+1}. \tag{3.2}$$

The natural ring homomorphism $\mu : R \to F = R/\mathfrak{m}$ gives an exact sequence of (multiplicative) Abelian groups,

$$1 \to 1 + \mathfrak{m} \to R^\times \to F^\times \to 1.$$

The Abelian group $F^\times$ is cyclic of order $q-1$, and $1+\mathfrak{m}$ has order q^j, which is relatively prime to $q-1$. It follows (from the structure theorem for finite Abelian groups, Theorem 1.1.16) that there is a splitting $\iota : F^\times \to R^\times$ and this gives the isomorphism (3.1). □

The structure of $1+\mathfrak{m}$ is often very complicated. However it is possible to identify the cyclic group $F^\times$ as a subgroup of $R^\times$.

Lemma 3.1.4. *There is a unique (group homomorphism) splitting $\iota : F^\times \to R^\times$ of the projection μ, and its image consists of all elements $\alpha \in R$ such that $\alpha^{q-1} = 1$.*

Proof. Every element $a \in F^\times$ satisfies $a^{q-1} = 1$ so if ι exists, the same must be true of $\iota(a)$. Let $g(x) = x^{q-1} - 1$. Then every element of $F^\times$ is a (simple) root of $\mu(g) \in F[x]$. Therefore g is a regular polynomial, and Lemma 3.1.1 implies that every element $a \in F^\times$ has a unique lift $\iota(a) \in R$ such that $\iota(a)^{q-1} = 1$. Hence the splitting ι exists, and there is only one such. □

3.2 Examples

3.2.a $\mathbb{Z}/(p^m)$

Fix a prime number $p \in \mathbb{Z}$ and let $R = \mathbb{Z}/(p^m)$. This is a finite local ring with maximal ideal $\mathfrak{m} = (p)$ and residue field $F = \mathbb{Z}/(p)$. The multiplicative group $F^\times$ is cyclic, of order $p-1$. By Proposition 3.1.3 the group of units $R^\times$ is the product $F^\times \times (1+\mathfrak{m})$.

Proposition 3.2.1. *If $p > 2$ then $1+\mathfrak{m}$ is a cyclic group of order p^{m-1} so $R^\times \cong \mathbb{Z}/(p-1) \times \mathbb{Z}/(p^{m-1}) \cong \mathbb{Z}/(p^{m-1}(p-1))$. If $p = 2$ and if $m \geq 3$ then $1+\mathfrak{m}$ is a product of two cyclic groups, one of order 2 (generated by the element -1), the other of order 2^{m-2} (generated by the element 5).*

Proof. The order of the group of units is easy to calculate: since every pth integer is a multiple of p, there are $p^m/p = p^{m-1}$ non-invertible elements in R. So there are $p^m - p^{m-1} = (p-1)p^{m-1}$ units. It follows that $1 + \mathfrak{m}$ contains p^{m-1} elements.

Now consider the case $p \geq 3$. Define $E : \mathbb{Z} \to R = \mathbb{Z}/(p^m)$ by $E(a) = \exp(pa) \pmod{p^m}$. That is,

$$E(a) = 1 + pa + \frac{p^2a^2}{2!} + \frac{p^3a^3}{3!} + \cdots \pmod{p^m} \tag{3.3}$$

Consider the nth term, $a^n p^n/n!$. The number $n!$ is not necessarily invertible in $\mathbb{Z}/(p^m)$ but the number $p^n/n!$ does make sense in $\mathbb{Z}/(p^n)$ if we interpret it to mean that the factor p^e which occurs in the prime decomposition of $n!$ should be canceled with the same factor p^e which occurs in the numerator. In fact, the prime p occurs in the prime decomposition of $n!$ fewer than $n/p + n/p^2 + n/p^3 \cdots = n/(p-1)$ times. Since it occurs in the numerator n times, it is possible to cancel all occurrences of p from the denominator. This leaves a denominator which is relatively prime to p and hence is invertible in $\mathbb{Z}/(p^m)$. It follows, moreover, that after this cancellation the numerator still has at least $n(p-2)/(p-1)$ factors of p. So if $n \geq m(p-1)/(p-2)$ the term $a^n p^n/n!$ is 0 in $\mathbb{Z}/(p^m)$. Therefore the sum (3.3) is finite.

Since $E(a+b) = E(a)E(b)$, the mapping E is a group homomorphism. Moreover $E(a) = 1$ if and only if a is a multiple of p^{m-1}. So E induces to an injective homomorphism

$$E : \mathbb{Z}/(p^{m-1}) \to 1 + \mathfrak{m}.$$

This mapping is also surjective because both sides have p^{m-1} elements.

Now consider the case $R = \mathbb{Z}/(2^m)$ with $m \geq 3$. The element $\{-1\}$ generates a cyclic subgroup of order 2. The element 5 generates a cyclic subgroup of order 2^{m-2}. To show this, first verify by induction that

$$5^{2^{m-3}} = (1+2^2)^{2^{m-3}} \equiv 1 + 2^{m-1} \pmod{2^m}$$

so this number is not equal to 1 in $\mathbb{Z}/(2^m)$. However

$$5^{2^{m-2}} \equiv (1+2^{m-1})^2 \equiv 1 \pmod{2^m}.$$

So 5 has order 2^{m-2} in R. Since -1 is not a power of 5 (mod 4) it is also not a power of 5 (mod 2^m). Therefore the product of cyclic groups $\langle -1 \rangle \langle 5 \rangle$ has order 2^{m-1}, and it consequently exhausts all the units. □

3.2.b $F[x]/(x^m)$

Let F be a finite field and let $R = F[x]/(x^m)$. Then R is a finite local ring with maximal ideal $\mathfrak{m} = (x)$ and with residue field F. The mapping $\mu : R \to F$ (which associates to each polynomial its constant term) takes $R^\times$ surjectively to $F^\times$. This mapping has a splitting $F^\times \to R^\times$ which assigns

to any nonzero $a \in F$ the polynomial $a+0x$. This gives an isomorphism $R^\times \cong F^\times \times (1+\mathfrak{m})$, where $1+\mathfrak{m}$ is the (multiplicative) group of all polynomials of the form $1+xh(x)$, $h(x)$ a polynomial of degree $\leq m-2$. (So we have recovered Proposition 3.1.3.) It is fairly difficult to determine the exact structure of the group $1+\mathfrak{m}$ but the following proposition describes its general form. Let $q = |F| = p^d$ with p prime.

Proposition 3.2.2. *The (multiplicative) group $1+\mathfrak{m}$ is isomorphic to a product of (additive) cyclic groups,*

$$1+\mathfrak{m} \cong \mathbb{Z}/(p^{r_1}) \times \cdots \times \mathbb{Z}/(p^{r_k}) \tag{3.4}$$

where each $r_i \leq \lceil \log_p(m) \rceil$ and where

$$\sum_{i=1}^{k} r_i = d(m-1).$$

Proof. The Abelian group $1+\mathfrak{m}$ is finite. It is thus isomorphic to a product of cyclic groups whose orders divide $|1+\mathfrak{m}| = q^{m-1}$ which is a power of p. This gives an abstract isomorphism (3.4). Counting the number of elements on each side of this equation gives

$$q^{m-1} = p^{r_1+\cdots+r_k}$$

so

$$d(m-1) = \sum_{i=1}^{k} r_i.$$

Let r be the smallest integer such that $p^r \geq m$. Then $y^{p^r} = 1$ for any $y \in 1+\mathfrak{m}$, because expressing $y = 1+xh(x)$ and computing in $F[x]$ we find that

$$y^{p^r} = 1 + x^{p^r} h^{p^r} \equiv 1 \pmod{x^m}.$$

Thus the cyclic groups occurring in (3.4) each have $r_i \leq r = \lceil \log_p(m) \rceil$. □

3.2.c $F[x]/(f^m)$

Let F be a finite field and let $f \in F[x]$ be an irreducible polynomial. Fix $m \geq 1$. The ring $R = F[x]/(f^m)$ is a finite local ring with maximal ideal (f) and with quotient field $K = F[x]/(f)$. The next result identifies the ring R with that of Section 3.2.b. Let

$$\mu : R = F[x]/(f^m) \to K = F[x]/(f)$$

be reduction modulo f. It is a surjective ring homomorphism.

Proposition 3.2.3. *There is a unique splitting of μ. That is, there is a unique injective ring homomorphism $\varphi : K \to R$ so that $\mu(\varphi(a)) = a$ for all $a \in K$. Moreover the mapping φ extends to a mapping $\varphi : K[y] \to R$ by setting $\varphi(y) = f$. The resulting mapping*

$$\bar{\varphi} : K[y]/(y^m) \to R$$

is an isomorphism of rings.

Proof. Let q denote the number of elements in F and let $Q = q^d$ denote the number of elements in K, where $d = \deg(f)$. First we show that the set

$$Z_m = \left\{ g \in F[x]/(f^m) : \ g^Q = g \right\}$$

is a *lift*[1] of the field K to R. It is therefore a candidate for the image of φ.

The set Z_m is closed under addition and multiplication, because if $g_1, g_2 \in Z_m$ then

$$(g_1 + g_2)^Q = g_1^Q + g_2^Q = g_1 + g_2.$$

Moreover the restriction $\mu : Z_m \to K$ is an injection, for if $g \in Z_m$ lies in the kernel of μ and if $\dot{g} \in F[x]$ is any lift of g, then f divides $\dot{g}$. However f^m divides $\dot{g}^Q - \dot{g} = (\dot{g}^{Q-1} - 1)(\dot{g})$. Since these two factors are relatively prime, it follows that f^m divides $\dot{g}$, which says that $g = 0$ in R. Now let us show that the restriction $\mu : Z_m \to K$ is surjective. Fix $a \in K$. We need to find $g \in Z_m$ so that $\mu(g) = a$. We use induction on m, and the case $m = 1$ holds trivially. So let m be arbitrary and consider the mapping

$$\mu_m : F[x]/(f^m) \to F[x]/(f^{m-1}).$$

By induction, there exists $g' \in F[x]/(f^{m-1})$ so that $(g')^Q = g'$ and so that g' maps to the given element $a \in K$, that is, $g' \pmod f = a$. Let $\dot{g}' \in F[x]$ be any lift of g' to $F[x]$. Then f^{m-1} divides $(\dot{g}')^Q - \dot{g}'$, or

$$(\dot{g}')^Q - \dot{g}' = f^{m-1}h$$

for some polynomial $h \in F[x]$. Set $g = \dot{g}' + hf^{m-1}$. Then

$$(g)^Q - g = (\dot{g}')^Q - \dot{g}' + h^Q f^{(m-1)Q} - hf^{m-1} = h^Q f^{(m-1)Q}$$

which is divisible by f^m. This says that the class $[g] \in F[x]/(f^m)$ lies in the set Z_m and that $g \pmod f = a$ as needed.

The splitting φ is unique because every element g in the image of a splitting must satisfy $g^Q = g$. This function $\varphi : K \to R.$ extends to a function $\varphi : K[y] \to R$ by mapping y to f. We

[1] If $\tau : A \to B$ is a set function, then a *lift* of a subset $C \subset B$ is a subset of $D \subset A$ that is mapped by τ one to one and onto C. A lift of an element $y \in B$ is an element $x \in A$ so that $\tau(x) = y$.

claim that the kernel of φ is (y^m) and that φ is onto. The kernel contains (y^m) since $f^m = 0$ in R. Let

$$g(y) = \sum_{i=0}^{m-1} g_i y^i$$

with $\varphi(g) = 0$. Thus

$$\sum_{i=0}^{m-1} g_i f^i = 0. \tag{3.5}$$

As a vector space over K the ring R has dimension m since $|R| = Q^m = |K|^m$. R is spanned over K by $\{1, f, f^2, \cdots, f^{m-1}\}$ (this can be proved by induction on m). Therefore these elements form a basis. As we have seen in the preceding paragraph, the projection $\mu_m : F[x]/(f^m) \to F[x]/(f^{m-1})$ takes Z_m to Z_{m-1} (both of which are lifts of the field K). Applying the projection μ_m to equation (3.5) gives

$$\sum_{j=0}^{m-2} g_j f^j = 0$$

and by induction we conclude that $g_0 = g_1 = \ldots = g_{m-2} = 0$. This leaves $g_{m-1} f^{m-1} = 0$ in the ring R, which means that f^m divides $g_{m-1} f^{m-1}$ in the polynomial ring $F[x]$. But $F[x]$ is an integral domain, so we conclude that f divides g_{m-1}, hence $g_{m-1} = 0$ as an element of K.

In conclusion, we obtain a well defined surjective ring homomorphism $K[y] \to R$ by sending y to f. The kernel of this homomorphism is the ideal (y^m) so we obtain an isomorphism $K[y]/(y^m) \to R$. □

3.2.d Equal characteristics

Suppose that R is a finite local ring with maximal ideal $\mathfrak{m}$ and quotient field $F = R/\mathfrak{m}$. Recall that there is a unique homomorphism $\mathbb{Z} \to R$ (taking m to $1 + \cdots + 1$, m times). Its kernel is an ideal $(t) \subset \mathbb{Z}$ where $t = \mathrm{char}(R)$ is the characteristic of R. Since R is finite, its characteristic is nonzero. If the characteristic of R were divisible by two distinct primes, say p and q, then neither p nor q would be a unit, hence both would be in $\mathfrak{m}$. It would follow that 1 is in $\mathfrak{m}$, since 1 is an integer linear combination of p and q. Hence $\mathrm{char}(R) = p^e$ is a power of a prime p. Moreover, the image of $\mathbf{Z}$ in F is a quotient of its image $\mathbf{Z}/(p^e)$ in R. Thus $\mathrm{char}(F) = p$.

Let $\mu : R \to F$ be the quotient mapping. Set $q = |F|$. Let $\iota : F^\times \to R^\times$ be the homomorphism described in Lemma 3.1.4. Extend ι to F by mapping 0 to 0.

Proposition 3.2.4. *The function $\iota : F \to R$ is a ring homomorphism if and only if R and F have the same characteristic (so $t = p$ and $e = 1$).*

Proof. Whenever $f : A \to B$ is a ring homomorphism, $\mathrm{char}(B)$ divides $\mathrm{char}(A)$ because the kernel of the homomorphism from $\mathbf{Z}$ to B contains the kernel of the homomorphism from $\mathbf{Z}$ to A. If ι is a ring homomorphism then $\mathrm{char}(R)|\mathrm{char}(F)$ so $e = 1$.

For the convese, suppose that R and F have the same characteristic, p. Since ι is multiplicative, to show that ι is a ring homomorphism we need only show that for every $a, b \in F$ we have $\iota(a) + \iota(b) = \iota(a + b)$. The polynomial $x^q - x$ is regular over F and has only simple roots. Thus $\iota(a)$ can be defined to be the unique element of R so that $\mu(\iota(a)) = a$ and that is a root of $x^q - x$. This element exists by Lemma 3.1.1. We have

$$\mu(\iota(a) + \iota(b)) = \mu(\iota(a)) + \mu(\iota(b)) = a + b = \mu(\iota(a + b)),$$

so that $\iota(a) + \iota(b)$ and $\iota(a + b)$ are congruent modulo $\mathfrak{m}$. Also,

$$(\iota(a) + \iota(b))^q = \iota(a)^q + \iota(b)^q = \iota(a) + \iota(b),$$

because $(x + y)^p = x^p + y^p$ in any ring of prime characteristic p. Thus $\iota(a) + \iota(b)$ is in the image of ι and must equal $\iota(a + b)$. □

Proposition 3.2.5. *Let R be a finite local ring with quotient field $F = R/\mathfrak{m}$. Then* $\mathrm{char}(R) = \mathrm{char}(F)$ *if and only if there exists r, k so that R is isomorphic to the quotient $F[x_1, x_2, \cdots, x_r]/I$ where I is an ideal that contains every monomial of degree $\geq k$.*

Proof. Suppose $\mathrm{char}(R) = \mathrm{char}(F)$. Use ι to identify F as a subring of R. Let M be a set of variables in one to one correspondence with the elements of $\mathfrak{m}$. Then $R \cong F[M]/I$, where I is the set of all polynomials in M that vanish when the elements of M are replaced by the corresponding elements of $\mathfrak{m}$. Since $\mathfrak{m}^k = (0)$ for some k, every monomial of degree $\geq k$ is contained in I. Conversely, if F is a finite field, M is a finite set of variables, and I is an ideal in $F[M]$ containing every monomial of degree $\geq k$, then $R = F[M]/I$ is a finite local ring with maximal ideal generated by M whose characteristic equals that of its quotient field. □

3.3 Divisibility in $R[x]$

Throughout this subsection, R denotes a finite local ring with $\mu : R \to F = R/\mathfrak{m}$ the projection to its residue field. Let $f, g \in R[x]$.

1. f is *nilpotent* if $f^n = 0$ for some $n \geq 0$.
2. f is a *unit* if there exists $h \in R[x]$ so that $fh = 1$.
3. f is *regular* if f is not a zero divisor.
4. f is *prime* if the ideal (f) is a proper prime ideal.
5. f is *irreducible element* if f is not a unit and, whenever $f = gh$ then g or h is a unit.

6. f and g are *coprime* if $R[x] = (f) + (g)$.

In [24] the following results are proven.

Theorem 3.3.1. *Let $f = a_0 + a_1 x + \cdots + a_d X^d \in R[x]$. Then*

1. *The following are equivalent:*
   (a) *f is a unit.*
   (b) *$\mu(f) \in F[x]$ is a unit.*
   (c) *a_0 is a unit and the remaining coefficients $a_1, \cdots, a_d$ are nilpotent.*
2. *The following are equivalent:*
   (a) *f is nilpotent.*
   (b) *$\mu(f) = 0$.*
   (c) *All the a_i are nilpotent.*
   (d) *f is a zero divisor.*
   (e) *there exists $a \neq 0$ in R such that $af = 0$.*
3. *The following are equivalent:*
   (a) *f is regular.*
   (b) *$\mu(f) \neq 0$.*
   (c) *a_i is a unit for some i $(0 \leq i \leq d)$.*
4. *f and g are coprime if and only if $\mu(f)$ and $\mu(g)$ are coprime. In this case, f^i and g^j are coprime for all $i, j \geq 1$.*
5. *If $\mu(f)$ is irreducible then f is irreducible. If f is irreducible then $\mu(f) = ag^n$ where $a \in F$ and $g \in F[x]$ is a monic irreducible polynomial.*
6. *(Euclidean algorithm) If $f \neq 0$ and if $g \in R[x]$ is regular then there exist (not necessarily unique) elements $q, r \in R[x]$ such that $\deg r < \deg g$ and $f = gq + r$.*
7. *If f and g are monic and regular and if $(f) = (g)$ then $f = g$.*

Recall that an ideal $I \subset R[x]$ is *primary* if $I \neq R[x]$ and whenever $ab \in I$, then either $a \in I$ or $b^n \in I$ for some $n \geq 1$. An element $g \in R[x]$ is primary if (g) is primary.

Proposition 3.3.2. *An element $f \in R[x]$ is a primary regular non-unit if and only if $f = ug^n + h$ where $u \in R[x]$ is a unit, $g \in R[x]$ is a basic irreducible, $n \geq 1$, and $h \in \mathfrak{m}[x]$ (that is, all the coefficients of h lie in $\mathfrak{m}$).*

Although $R[x]$ is not necessarily a unique factorization domain, the following theorem ([24] Thm. XIII.11) states that regular polynomials have unique factorization.

Theorem 3.3.3. *Let $f \in R[x]$ be a regular polynomial. Then there exist unique (up to reordering and multiplication by units) regular coprime primary polynomials $g_1, g_2, \cdots, g_n \in R[x]$ so that $f = g_1 g_2 \cdots g_n$.*

3.4 Tools for local rings

In this section we develop several tools for the analysis of finite local rings – Galois theory, the trace and norm, and primitive elements. These are all generalizations of the similarly named tools for analyzing finite fields, and in most cases we use the finite field versions to help construct the finite local ring version.

3.4.a Galois theory of local rings

In the next few paragraphs we see that a finite local ring R has a distinguished collection of *Galois extensions* $\mathrm{GR}(R, n)$, one for each positive integer n, which are themselves local rings and for which many of the familiar properties of Galois fields continue to hold.

Extensions. Let R be a finite local ring. An *extension* ring is a finite local ring S which contains R. Any extension S of R is an R-algebra. A ring homomorphism $\varphi : S \to S$ is said to be an R-algebra automorphism of S provided it is both surjective and injective, and provided $\varphi(ac) = a\varphi(c)$ for all $a \in R$ and $c \in S$. Define the *Galois group*

$$G = \mathrm{Gal}(S/R) = \mathrm{Aut}_R(S)$$

to be the set of R-algebra automorphisms of S. The Galois group G acts on S. Let S^G denote the set of elements which are fixed under the action of G (hence $R \subset S^G$). Then S^G is an R-algebra. If $\mathfrak{M}$ is the maximal ideal of S, then S^G is a finite local ring with maximal ideal $S^G \cap \mathfrak{M}$, hence is an extension of R. An extension S of R is *unramified* if the maximal ideal $\mathfrak{m}$ of R generates the maximal ideal of S; otherwise it is said to be *ramified* If S is an unramified extension of R then $\mathfrak{m}^i$ generates $\mathfrak{M}^i$ so the degree of nilpotency of $\mathfrak{m}$ equals the degree of nilpotency of $\mathfrak{M}$. An unramified extension $R \subset S$ is said to be a *Galois extension* if $R = S^G$.

Example Let R be a finite local ring with maximal ideal $\mathfrak{m}$. Let $f \in R[x]$ be a monic basic irreducible polynomial. The extension $S = R[x]/(f^m)$ is again a finite local ring (see Section 3.1). Its maximal ideal is $\mathfrak{M} = \mathfrak{m} + (f)$. If $m > 1$ then S is a *ramified* extension of R. If $m = 1$ then S is an unramified extension and $\mathfrak{M} = \mathfrak{m}S$ is generated by $\mathfrak{m}$.

The following result is the main theorem in the Galois theory of finite local rings. The proof may be found in [24].

Theorem 3.4.1. *Let R be a finite local ring. Then every unramified extension $R \subset S$ is a Galois extension. Suppose $R \subset S$ is such an extension, with corresponding maximal ideals $\mathfrak{m} \subset \mathfrak{M}$. Then*

the following diagram

$$\begin{array}{ccc} S & \xrightarrow{\nu} & K = S/\mathfrak{M} \\ \bigcup & & \bigcup \\ R & \xrightarrow{\mu} & F = R/\mathfrak{m} \end{array} \tag{3.6}$$

induces an isomorphism $Gal(S/R) \cong Gal(K/F)$ *which is therefore a cyclic group. There exists* $h \in S$ *so that* $S = R[h]$*. The mapping determined by* $h \mapsto h^{|F|}$ *generates* $Gal(S/R)$*. Let* $h = h_1, h_2, \ldots, h_d$ *be the distinct images of* h *under* $Gal(S/R)$*. Then the following polynomial*

$$f(x) = (x - h_1)(x - h_2) \cdots (x - h_d) \tag{3.7}$$

actually lies in $R[x]$*. It is a (monic) basic irreducible polynomial of degree* $d = |Gal(S/R)|$*. The mapping* $R[x]/(f) \to S$ *which takes* $x \in R[x]$ *to* $h \in S$ *is an isomorphism of rings (and of* R*-algebras). The ring* S *is a free module of rank* d *over the ring* R*, hence* $|S| = |R|^d$ *and we say that* S *is an extension of* degree d*. The above diagram induces a (combinatorial) lattice preserving bijection between the Galois extensions of* R *which are contained in* S *and the field extensions of* F *which are contained in* K*. The ring* S *is a field if and only if the ring* R *is a field. If* $f' \in R[x]$ *is another monic basic irreducible polynomial of the same degree* d *then there exists an* R*-algebra isomorphism* $S \cong R[x]/(f')$*. In particular,* f' *also splits into linear factors over* S*.*

Corollary 3.4.2. *Let* R *be a finite local ring, let* S *be an unramified degree* d *extension of* R*, and let* $f \in R[x]$ *be a monic basic irreducible polynomial of degree* d*. Let* $\alpha \in S$ *be a root of* f*. Then the collection*

$$\left\{1, \alpha, \alpha^2, \cdots, \alpha^{d-1}\right\}$$

is a basis of S *over* R*. The element* α *is invertible in* S*.*

Proof. According to Theorem 3.4.1, we may replace S with $R[x]/(f)$ and we may replace α with x. By the division theorem for polynomials, the set

$$\left\{1, x, x^2, \cdots, x^{d-1}\right\}$$

is a basis of $R[x]/(f)$ over R. If $f(x) = a_0 + a_1x + \cdots + a_dx^d$ then $\mu(a_0) \neq 0$ since $\mu(f)$ is irreducible. Therefore a_0 is invertible in S and

$$x^{-1} = \frac{-1}{a_0}(a_1 + a_2x^2 + \cdots + a_dx^{d-1})$$

in $R[x]/(f)$. □

3.4.b The Trace and the norm

Let $R, \mathfrak{m}, F = R/\mathfrak{m}$ be a finite local ring with $\mu : R \to F$ the reduction map. Let $S, \mathfrak{M}, K = S/\mathfrak{M}$ be a Galois extension of degree d with $\nu : S \to K$ the reduction map. Let $a \in S$. The *trace* $\mathsf{Tr}_{S/R}(a) \in R$ and *norm* $N_{S/R}(a) \in R$ of a are defined to be

$$\mathsf{Tr}_{S/R}(a) = \sum_{\sigma \in \mathrm{Gal}(S/R)} \sigma(a)$$

and

$$N_{S/R}(a) = \prod_{\sigma \in \mathrm{Gal(S/R)}} \sigma(a).$$

Consider the mapping $\kappa_a : S \to S$ which is given by multiplication by a. Since S is a free module over R it has a basis consisting of d elements, and the mapping κ_a may be expressed as a $d \times d$ matrix M_a. Then the trace and norm of a equal the trace and determinant (respectively) of this matrix (which are thus independent of the choice of basis).

Lemma 3.4.3. *$\mathsf{Tr}_{S/R}(a)$ equals the trace of M_a and $N_{S/R}(a)$ equals the determinant of M_a. Also, we have $\mu \circ \mathsf{Tr}_{S/R} = \mathsf{Tr}_{K/F} \circ \nu$ and $\mu \circ N_{S/R} = N_{K/F} \circ \nu$.*

Proof. The last statement of the theorem follows from Theorem 3.4.1. We know the first statement concerning the trace is true for the fields K and F by Proposition 2.2.14. Let N be the set of elements a of S such that the trace of a equals the trace of M_a. Then N is an R-submodule of S since the mapping from a to the trace of M_a is R-linear. Moreover $S = N + \mathfrak{M}S = N + \mathfrak{m}S$. By Nakayama's lemma (Theorem 3.1.2) we have $S = N$, which proves the claim.

Next we consider the norm. Let us denote the determinant of M_a by $D(a)$. We want to show that $D(a) = N_{S/R}(a)$ for every $a \in S$. Since both $N_{S/R}$ and D are multiplicative, it suffices to show this for a set V such that every element of S is a product of elements of V.

If $a \in R$, then $M_a = aI$ so $D(a) = a^d$, and $N_{S/R}(a) = a^d$.

Suppose that $a \in S$ reduces to a primitive element of K modulo $\mathfrak{M}$. If N is the R-submodule of S spanned by $1, a, \cdots, a^{d-1}$, then $S = N + \mathfrak{M}$, so by Nakayama's lemma $S = N$. That is, $1, a, \cdots, a^{d-1}$ is an R-basis for S. With respect to this basis M_a has the form described in the proof of Proposition 2.2.14. If

$$f(x) = x^d + \sum_{i=0}^{e/d-1} a_i x^i$$

is the minimal polynomial of a over R, then $D(a) = a_0 = N_{S/R}(a)$. Thus $D(a^i) = N_{S/R}(a^i)$ for every i. If n is the degree of nilpotency of S and R, then $|S| = |K|^n$. We have thus far accounted for the $(|K| - 2)|K|^{n-1}$ elements of S that are congruent to some a^i, $i = 1, \cdots, |K| - 2$. We also

have $D((a+b)/a) = N_{S/R}((a+b)/a)$ if $b \in \mathfrak{M}$. This accounts for the $|\mathfrak{M}| = |K|^{n-1}$ elements in $1+\mathfrak{M}$, and hence for all the units. Finally, since $\mathfrak{M} = \mathfrak{m}S$, every element of $\mathfrak{M}$ can be written in the form cb with $c \in \mathfrak{m}^i$ for some i and b a unit. Using multiplicativity again completes the proof. □

Corollary 3.4.4. *The trace $\mathsf{Tr}_{S/R} : S \to R$ is surjective.*

Proof. First we show there exists an element $s \in S$ so that $\mathsf{Tr}(s)$ is invertible in R. If this were false, then we would have $\mathsf{Tr}(s) \in \mathfrak{m}$ for all $s \in S$ which would imply that the induced mapping $S/\mathfrak{M} \to R/\mathfrak{m}$ is 0. This would contradict the above lemma which states that this induced mapping is the trace, $\mathsf{Tr}_{K/F}$, which is surjective. So choose $c \in S$ so that $\mathsf{Tr}_{S/R}(c)$ is invertible and let $a \in R$ denote its inverse. Then for any $b \in R$ we have $\mathsf{Tr}_{S/R}(bac) = baTr_{S/R}(c) = b$. □

Theorem 3.4.5. *Let $\sigma \in Gal(S/R)$ be a generator of the Galois group. Then $\mathsf{Tr}_{S/R}(a) = 0$ if and only if there exists $c \in S$ such that $a = c - \sigma(c)$, and $N_{S/R}(a) = 1$ if and only if there is a unit $b \in S$ so that $a = b\sigma(b)^{-1}$.*

Proof. The ring S is a free module over R of rank d. First we prove the statement about the trace. Let $\phi : S \to S$ be defined by $\phi(x) = x - \sigma(x)$. The kernel of ϕ is R since S is a Galois extension of R. As a homomorphism of R modules the rank of ϕ is $d-1$ because its kernel is 1-dimensional. Therefore the image of ϕ contains $|R|^{d-1}$ elements. The image of ϕ is contained in Ker(Tr) which by Corollary 3.4.4 also contains $|R|^{d-1}$ elements, so they coincide. Thus $Tr(a) = 0$ if and only if $a = b - \sigma(b)$ for some $b \in S$.

The statement concerning the norm is similar, but it uses the function $\psi : S^\times \to S^\times$ defined by $\psi(x) = x\sigma(x)^{-1}$. □

Suppose $L : S \to R$ is any R-linear mapping. Then for any $i \geq 1$ we have $L(\mathfrak{M}^i) \subset \mathfrak{m}^i$. (Since $\mathfrak{M} = \mathfrak{m}S$, any element in $\mathfrak{M}^i$ may be expressed as ac with $a \in \mathfrak{m}^i$ and $c \in S$, in which case $L(ac) = aL(c) \in \mathfrak{m}^i$.) In particular, L induces an F-linear mapping $\bar{L} : K = S/\mathfrak{M} \to F = R/\mathfrak{m}$ and the diagram

$$\begin{array}{ccc} S & \xrightarrow{\nu} & K = S/\mathfrak{M} \\ {\scriptstyle L}\downarrow & & \downarrow{\scriptstyle \bar{L}} \\ R & \xrightarrow{\mu} & F = R/\mathfrak{m} \end{array} \tag{3.8}$$

commutes. Let us say that L is *nonsingular* if this mapping $\bar{L}$ is surjective. This is equivalent to saying that $\bar{L}$ is not the zero map.

Theorem 3.4.6. *Let $L : S \to R$ be an R linear mapping. Then*

1. *The mapping $L : S \to R$ is surjective if and only if L is nonsingular. (In particular, the trace $\mathsf{Tr}_{S/R}$ is nonsingular.)*

2. *If L is nonsingular, then $L(\mathfrak{M}^i) = \mathfrak{m}^i$ for any $i \geq 1$.*
3. *If L is nonsingular, $b \in S$ and $L(ab) = 0$ for all $a \in S$, then $b = 0$.*
4. *There exists $b \in S$ so that $L(a) = \mathsf{Tr}(ba)$ for all $a \in S$. The element b is invertible if and only if L is nonsingular.*

Proof. If L is surjective then it is nonsingular by diagram (3.8). On the other hand, if L is nonsingular then (as above) there exists $b \in S$ such that $L(b)$ is invertible in R. If $a = L(b)^{-1}$ then, for any $c \in R$, $L(cab) = c$ so L is surjective. This proves (1). We already know that $L(\mathfrak{M}^i) \subset \mathfrak{m}^i$ so let $c \in \mathfrak{m}^i$ and, by part (1), let $a_0 \in S$ be an element such that $L(a_0) = 1$. Then $ca_0 \in \mathfrak{M}^i$ and $L(ca_0) = c$, which proves (2).

To prove (3), let n be the degree of nilpotency of $\mathfrak{m}$. That is, $\mathfrak{m}^n = 0$ but $\mathfrak{m}^{n-1} \neq 0$. Then n is also the degree of nilpotency of $\mathfrak{M}$. Let $b \neq 0 \in S$ and suppose that $L(ab) = 0$ for all $a \in S$. Let $m < n$ be the largest integer so that $b \in \mathfrak{M}^m$. Then $b = db_1$ with $d \in \mathfrak{m}^m - \mathfrak{m}^{m+1}$ and b_1 a unit in S. Therefore for all $a \in S$ we have $0 = L(da) = dL(a)$. But $m < n$ so we must have $L(a) \in \mathfrak{M}$ which contradicts the nonsingularity of L, proving (3).

To prove (4), consider the mapping $S \to \mathrm{Hom}_R(S, R)$ which assigns to any $b \in S$ the R linear mapping $a \mapsto \mathsf{Tr}_{S/R}(ab)$. This mapping is injective, for if $b' \in S$ and $\mathsf{Tr}_{S/R}(ab) = \mathsf{Tr}_{S/R}(ab')$ for all $a \in S$, then by part (3) this implies $b = b'$. Since S is a free module over R of some rank d, there are $|R|^d$ elements in $\mathrm{Hom}_R(S, R)$. But this is the same as the number of elements in S. Therefore every R-linear mapping $L : S \to R$ is of the form $a \mapsto \mathsf{Tr}_{S/R}(ab)$ for some $b \in S$. If b is invertible, then the mapping L is nonsingular, whereas if $b \in \mathfrak{M}$ then $L(ab) \in \mathfrak{m}$ so the resulting mapping $\bar{L} : S/\mathfrak{M} \to R/\mathfrak{m}$ is zero. □

3.4.c Primitive polynomials

Let R be a finite local ring with maximal ideal $\mathfrak{m}$ and residue field $\mu : R \to F = R/\mathfrak{m}$. Let S be a degree d Galois extension of R, with maximal ideal $\mathfrak{M}$ and residue field $\nu : S \to K = S/\mathfrak{M}$ as in (3.6). Let $f \in R[x]$ be a basic irreducible polynomial of degree d. Then f is said to be *primitive* if the polynomial $\bar{f} = \mu(f) \in F[x]$ is primitive. That is, if for some (and hence for any) root $\bar{a} \in K$ of $\bar{f}$, the distinct powers of $\bar{a}$ exactly account for all the nonzero elements in K. Unfortunately this is not enough to guarantee that each root $a \in S$ of f generates the cyclic group $\iota(K^\times) \subset S$.

Lemma 3.4.7. *Let $f \in R[x]$ be a basic irreducible polynomial of degree d and let S be a degree d Galois extension of R, so that f splits into linear factors over S. Let $a \in S$ be a root of f. If $\mu(f)$ is primitive (in $F[x]$) then the elements $\{1, a, a^2, \cdots, a^{Q-2}\}$ are distinct, where $Q = |K| = |F|^d$. The roots of f lie in $\iota(K^\times) \subset S^\times$ if and only if f divides $x^Q - 1$. Thus, if $\mu(f)$ is primitive and f divides $x^Q - 1$, then $\iota(K^\times) \subset S^\times$ consists of the $Q - 1$ distinct powers $\{1, a, a^2, \cdots, a^{Q-2}\}$ of a.*

Proof. The element $\mu(a) \in K$ is a root of $\mu(f) \in F[x]$. If $\mu(f)$ is primitive, then $\mu(a)$ is a primitive element in K and the elements $\mu(a)^i$ $(0 \leq i \leq Q-2)$ are distinct, so the same is true of the elements

a^i $(0 \le i \le Q-2)$. By 3.1.4 the polynomial $g(x) = x^{Q-1} - 1$ factors completely in S as

$$g(x) = \prod_{b \in K^\times} (x - \iota(b)).$$

Since f also factors completely over S, we see that the roots of f lie in $\iota(K^\times)$ if and only if f divides $g(x)$. □

3.5 Galois rings

Let $p \in \mathbb{Z}$ be a prime number. According to Theorem 3.4.1, for each $n, d \ge 1$ the ring $\mathbb{Z}/(p^n)$ has a unique Galois extension of degree d. This extension $S = GR(p^n, d)$ is called the *Galois ring* of degree d over $\mathbb{Z}/(p^n)$. For $n = 1$ it is the Galois field $\mathbb{F}_{p^d}$. For $d = 1$ it is the ring $\mathbb{Z}/(p^n)$. Let us review the general facts from Section 3.4 for the case of a Galois ring S.

The Galois ring $S = GR(p^n, d)$ is isomorphic to the quotient ring $\mathbb{Z}/(p^n)[x]/(f)$ where $f \in \mathbb{Z}/(p^n)[x]$ is a monic basic irreducible polynomial. That is, it is a monic polynomial such that its reduction $f \pmod p \in \mathbb{Z}/(p)[x]$ is irreducible. The ring S contains p^{nd} elements. For each divisor e of d the Galois ring S contains the ring $GR(p^n, e)$ and this accounts for all the subrings of S. For any $m \le n$ there is a projection $S \to GR(p^m, d)$ whose kernel is the ideal (p^m), and this accounts for all the nontrivial ideals in S. In particular the maximal ideal $\mathfrak{M} = (p) = pS$ consists of all multiples of p. The quotient $S/\mathfrak{M} \cong \mathbb{F}_{p^d}$ is isomorphic to the Galois field with p^d elements. If μ denotes the projection to this quotient, then it is compatible with the trace mapping in the sense that the following diagram commutes,

$$\begin{array}{ccc} S = GR(p^n, d) & \xrightarrow{\mu} & K = \mathbb{F}_q \\ \mathsf{Tr}\downarrow & & \downarrow\mathsf{Tr} \\ \mathbb{Z}/(p^n) & \xrightarrow[\mu]{} & \mathbb{F}_p \end{array}$$

where $q = p^d$. There is a natural (multiplication-preserving) splitting $\iota : K \to S$ of the mapping μ whose image is the set all elements $x \in S$ such that $x^q = x$. The group of units of S is the product

$$S^\times = \iota(K^\times) \times (1 + \mathfrak{M}).$$

If $p \ge 3$ then

$$1 + \mathfrak{M} \cong \mathbb{Z}/(p^{n-1}) \times \cdots \times \mathbb{Z}/(p^{n-1}) \quad (d \text{ times}).$$

If $p = 2$ and $n \ge 3$ then

$$1 + \mathfrak{M} \cong \big(\mathbb{Z}/(2^{n-1})\big)^{d-1} \times \mathbb{Z}/(2^{n-2}) \times \mathbb{Z}/(2)$$

If $p = 2$ and $n = 1, 2$ then in this equation, each factor $\mathbb{Z}/(2^m)$ should be dropped whenever $m \leq 0$.

It follows that, in general, $S^\times$ contains cyclic subgroups of order $(p^d - 1)p^{n-1}$ and that $|S^\times| = (p^d - 1)p^{d(n-1)}$.

Lemma 3.5.1. *For any $x \in S$ there are unique elements $a_0, a_1, \cdots, a_{n-1} \in \iota(K)$ such that*

$$x = a_0 + a_1 p + \cdots + a_{n-1} p^{n-1}. \tag{3.9}$$

The coefficients $a_0, a_1, \cdots a_{n-1}$ in (3.9) are called the coordinates *of x, and the expansion (3.9) is called the p-*adic expansion *of x.*

Proof. First note that if $t \in \iota(K)$ and if $1 - t$ is not a unit, then $t = 1$. Next, according to the comments in the first paragraph of this section, $|\mathfrak{M}^i/\mathfrak{M}^{i+1}| = q$ for $1 \leq i \leq n-1$. We claim that every element of $\mathfrak{M}^i/\mathfrak{M}^{i+1}$ has a unique representative of the form ap^i where $a \in \iota(K)$. Certainly $ap^i \in \mathfrak{M}^i$ and there are no more than q such elements, so we need to show these elements are distinct modulo $\mathfrak{M}^{i+1}$. Suppose $ap^i \equiv bp^i \pmod{\mathfrak{M}^{i+1}}$ with $a, b \in \iota(K)$. Then $p^i(1 - ba^{-1}) \in \mathfrak{M}^{i+1}$ from which it follows that $1 - ba^{-1} \in \mathfrak{M}$. But $ba^{-1} \in \iota(K)$ so the above note implies that $a = b$.

It now follows by induction that every $x \in \mathfrak{M}^i$ has a unique expression $x = p^i(a_0 + a_1 p + \cdots + a_{n-i-1}p^{n-i-1})$ with $a_i \in \iota(K)$. The coefficient a_0 is the unique representative of $x \pmod{\mathfrak{M}^{i+1}}$, while the inductive step applies to $x - p^i a_0 \in \mathfrak{M}^{i+1}$. □

The advantage of Lemma 3.5.1 is that multiplication by elements in $\iota(K)$ is described coordinatewise. That is, if $b \in \iota(K)$ and if x is given by 3.9, then $ba_0 + ba_1 p + \cdots + ba_{n-1}p^{n-1}$ is the p-adic expansion of bx. Multiplication by p is given by a "shift" of the coefficients a_i. However addition is described using a generalized "carry" procedure: if $a, b \in \iota(K)$ and if $a+b = c_0+c_1 p+\cdots+c_{n-1}p^{n-1}$ is the p-adic expansion of $a + b$ then we may think of the coefficient c_0 as the "sum" and the coefficients c_i (for $i \geq 1$) as being higher "carries".

3.6 Exercises

1. Let R be a finite local ring with maximal ideal $\mathfrak{m}$. Show that

   a.the ideal $\mathfrak{m}$ consists precisely of the non-units of R,
   b.for every $a \in R$, at least one of a and $1 + a$ is a unit, and
   c.there is a positive integer n such that $\mathfrak{m}^n = 0$.

2. Let R be a finite local ring with maximal ideal $\mathfrak{m}$ and residue field $F = R/\mathfrak{m}$. Show that $\mathfrak{m}^{i-1}/\mathfrak{m}^i$ naturally admits the structure of a vector space over F.

3. If R is a local ring and $g \in R[x]$ is regular, then use Nakayama's Lemma to show that for every $f \in R[x]$ there exist $q, r \in R[x]$ with $f = gq + r$ and $\deg(r) < \deg(g)$.

4. Show that for $p = 3$ and $m = 3$, the mapping $E : \mathbb{Z}/(3^2) \to \mathbb{Z}/(3^3)$ of Section 3.2.a is given by

$$E(a) = 1 + 3a + 18a^2 + 18a^3.$$

5. Let S/R be a Galois extension of finite local rings $\sigma \in \mathrm{Gal}(S/R)$ be a generator of the Galois group. Prove that $N_{S/R}(a) = 1$ if and only if there is a unit $b \in S$ so that $a = b\sigma(b)^{-1}$.

Chapter 4 Sequences, Power Series and Adic Rings

The central theme of this work is the design and analysis of sequences by identifying them with algebraic structures. The most common example associates to a sequence $\mathbf{a}$ its *generating function*, the formal power series whose coefficients are the elements of the sequence. This idea has been extremely fruitful, with applications to many disparate areas including probability theory, cryptography, combinatorics, random number generation, and algebraic topology. However, an infinite sequence may also be associated to a p-adic number, a π-adic number, or a reciprocal power series. Despite their differences, these algebraic structures can all be described in terms of a single general construction known as "completion". In this chapter these structures are individually described and an outline of the general theory is given.

4.1 Sequences

In this section we describe basic combinatorial notions concerning sequences.

4.1.a Periodicity

Let A be a set and let $\mathbf{a} = (a_0, a_1, a_2, \cdots)$ be a sequence of elements $a_i \in A$, also called a *sequence over* A. If the set A is discrete (meaning that it is finite or countable) then we refer to A as the *alphabet* from which the *symbols* a_i are drawn. If N is a natural number and $A = \{0, 1, \cdots, N-1\}$, then we refer to $\mathbf{a}$ as an N*-ary sequence*. The sequence $\mathbf{a}$ is *periodic* if there exists an integer $T > 0$ so that

$$a_i = a_{i+T} \tag{4.1}$$

for all $i = 0, 1, 2, \cdots$. Such a T is called *a period* of the sequence $\mathbf{a}$ and the least such T is called *the period*, or sometimes the *least period* of $\mathbf{a}$. The sequence $\mathbf{a}$ is *eventually periodic* if there exists $N > 0$ and $T > 0$ so that equation (4.1) holds for all $i \geq N$. To emphasize the difference, we sometimes refer to a periodic sequence as being *purely periodic* or *strictly periodic*. A *period* (resp. the *least period*) of an eventually periodic sequence refers to a period (resp. least period) of the periodic part of $\mathbf{a}$.

Lemma 4.1.1. *Suppose* $\mathbf{a}$ *is a periodic (or eventually periodic) sequence with least period* T*. Then every period of* $\mathbf{a}$ *is a multiple of* T*.*

Proof. If T' is a period of $\mathbf{a}$, then dividing by T gives $T' = qT + r$ for some quotient $q \geq 1$ and remainder r with $0 \leq r \leq T - 1$. Since both T and T' are periods, $a_{i+T'} = a_{i+qT+r} = a_{i+r}$ for all $i \geq 0$. Therefore r is a period also. Since $r < T$, the minimality of T implies $r = 0$. □

4.1.b Distinct sequences

Let A be an alphabet and let $\mathbf{a} = (a_0, a_1, \cdots)$ and $\mathbf{b} = (b_0, b_1, \cdots)$ be sequences of elements of A. We say that $\mathbf{b}$ is a *shift* of $\mathbf{a}$ if there exists $\tau \geq 0$ so that $b_i = a_{i+\tau}$ for all $i \geq 0$. We write $\mathbf{b} = \mathbf{a}^\tau$. If no such shift τ exists then we say that $\mathbf{a}$ and $\mathbf{b}$ are *shift distinct*. If $\mathbf{a}$ and $\mathbf{b}$ are periodic with the same period and $\mathbf{b}$ is a shift of $\mathbf{a}$, then we say that $\mathbf{b}$ is a *left shift* of $\mathbf{a}$. If no such shift exists then $\mathbf{a}$ and $\mathbf{b}$ are *shift distinct*. More generally, if $\mathbf{a}$ is a sequence over an alphabet A and $\mathbf{b}$ is a sequence over an alphabet B, we say that $\mathbf{a}$ and $\mathbf{b}$ are *isomorphic* if there exists an isomorphism of sets $\sigma : A \to B$ so that $b_i = \sigma(a_i)$ for all $i \geq 0$. (If $A = B$ are the same alphabet then σ is just a permutation of the symbols in the alphabet.) We say the sequences $\mathbf{a}$ and $\mathbf{b}$ are *isomorphic up to a shift* if there exists an isomorphism $\sigma : A \to B$ and a shift τ such that $b_i = \sigma(a_{i+\tau})$ for all $i \geq 0$. If no such pair σ, τ exists then we say that $\mathbf{a}$ and $\mathbf{b}$ are *non-isomorphic, even after a shift*.

4.1.c Sequence generators and models

The sequences described in this book are generated by algebraic methods involving rings. We formalize constructions of this type by defining a *sequence generator*. In the models we encounter, the state space of the sequence generator usually corresponds to a cyclic subgroup of the group of units in a ring.

Definition 4.1.2. *A* sequence generator*, or* discrete state machine with output

$$F = (U, \Sigma, f, g)$$

consists of a set U of states*, an alphabet Σ of* output values*, a state transition function $f : U \to U$ and an output function $g : U \to \Sigma$.*

Such a generator is depicted as follows:

$$f \circlearrowright U \xrightarrow{\text{g}} \Sigma.$$

The set U of states is assumed to be *discrete*, meaning that it is either finite or countably infinite. We also assume the alphabet Σ of possible output values is discrete. Given an initial state $\mathbf{s} \in U$, such a sequence generator outputs an infinite sequence

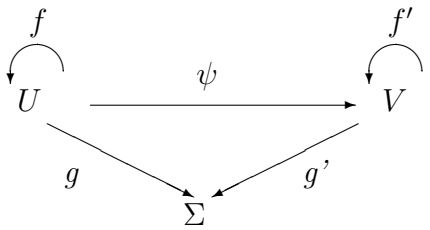
$$F(\mathbf{s}) = g(\mathbf{s}), g(f(\mathbf{s})), g(f^2(\mathbf{s})), \cdots$$

with elements in Σ. A state $\mathbf{s} \in U$ is *aperiodic* if, starting from $\mathbf{s}$, the generator never returns to this state. The state $\mathbf{s}$ is *periodic* of period L if starting from $\mathbf{s}$, after L steps, the generator returns to the state $\mathbf{s}$. That is, if $f^L(\mathbf{s}) = \mathbf{s}$. The *least period* of such a periodic state is the least

such $L \geq 1$. A state $\mathbf{s}$ is *eventually periodic* if, starting from $\mathbf{s}$, after a finite number of steps, the generator arrives at a periodic state. If U is finite then every state is eventually periodic. We say a set of states is *closed* if it is closed under state change. It is *complete* if it consists of all the periodic states. If a state $\mathbf{s}$ is periodic (resp., eventually periodic), then the output sequence $F(\mathbf{s})$ is periodic (resp., eventually periodic) as well. The converse is false, however. For example, let $F = (\mathbb{N}, \{0,1\}, f, g)$ with $f(n) = n+1$ and $g(n) = 0$ for all n. Then the output sequence from every state is periodic but no state is even eventually periodic.

Definition 4.1.3. *Let $F = (U, \Sigma, f, g)$ and $G = (V, \Sigma, f', g')$ be sequence generators. A* homomorphism *from F to G is a partial function ψ from U to V so that*

1. *for all $\mathbf{s} \in U$, if a is in the domain of ψ, then $f(a)$ is also in the domain of ψ, and*
2. *the following diagram commutes:*



That is, $g'(\psi(a)) = g(a)$ and $\psi(f(a)) = f'(\psi(a))$ for all a in the domain of ψ.

If R is a ring and $b \in R$, then let $h_b : R \to R$ denote multiplication by b. That is, $h_b(x) = bx$. Then for any function $T : R \to \Sigma$, the 4-tuple $R^{b,T} = (R, \Sigma, h_b, T)$ is a sequence generator.

Definition 4.1.4. *Let $F = (U, \Sigma, f, g)$ be a sequence generator. An* algebraic model *or simply a* model *for F is a homomorphism ψ of sequence generators between F and $R^{b,T}$ for some ring R, $b \in R$, and $T : R \to \Sigma$. The model is* injective *if $\psi : R^{b,T} \to F$ and the model is* projective *if $\psi : F \to R^{b,T}$.*

In the case of an injective model, if a is in the domain of ψ, then the output sequence generated from $\psi(a)$ is described by the *exponential representation*,

$$T(a), T(ba), T(b^2a), \cdots.$$

In the case of a projective model, if $\mathbf{s}$ is in the domain of ψ, then the output sequence generated from b is described by the *exponential representation*,

$$T(\psi(\mathbf{s})), T(b\psi(\mathbf{s})), T(b^2\psi(\mathbf{s})), \cdots.$$

If the ring R is a finite field, then every such sequence is strictly periodic (because $b^k a = b^{k+r} a$ implies that $a = b^r a$). We say that the model is *complete* if every periodic state $\mathbf{s} \in \Sigma$ is in the range (in the injective case) or domain (in the projective case) of ψ. A complete model, if one exists, allows us to analyze the behavior of the sequence generator using the algebraic structure of the ring R. In this book we encounter many different types of sequence generators and their models.

If ψ is a one to one mapping on its domain, then it can be inverted (possibly resulting in a partial function), allowing us to replace a projective model with an injective model, or vice versa. In practice, however it may require a nontrivial amount of computation to describe the inverse mapping, particularly when attempting to describe the initial state of the generator. Thus one or the other version may be a more natural way to describe a model.

4.2 Power series

4.2.a Definitions

Throughout this section we fix a commutative ring R (with identity 1).

Definition 4.2.1. *A (formal)* power series over R *is an infinite expression*

$$a(x) = a_0 + a_1 x + a_2 x^2 + \cdots,$$

where x is an indeterminate and $a_0, a_1, \cdots \in R$. As with polynomials, the a_is are called coefficients. *The sequence $(a_0, a_1, \cdots)$ of coefficients of a power series $a(x)$ is denoted* $\mathbf{seq}(a)$. *If $b(x) = b_0 + b_1 x + b_2 x^2 + \cdots$ is a second power series over R, then define*

$$(a+b)(x) = a(x) + b(x) = \sum_{i=0}^{\infty} (a_i + b_i) x^i$$

and

$$(ab)(x) = a(x)b(x) = \sum_{i=0}^{\infty} (\sum_{j=0}^{i} a_j b_{i-j}) x^i.$$

The set of power series over R is denoted $R[[x]]$. The least degree *of a nonzero power series $a(x) = \sum_{i=0}^{\infty} a_i x^i$ is the least index i such that $a_i \neq 0$. The least degree of 0 is ∞.*

These operations make $R[[x]]$ into a ring with identity given by the power series $1 = 1 + 0x + 0x^2 + \cdots$. The following lemma concerns a remarkable property of the ring of power series: most elements have inverses in $R[[x]]$ and it is easy to determine when an element is invertible.

Lemma 4.2.2. *Let $b(x) = \sum_{i=0}^{\infty} b_i x^i \in R[[x]]$ be a power series. Then (1) b is invertible in $R[[x]]$ if and only if (2) the constant term $b_0 \in R$ is invertible in R.*

Proof. The constant term of a product is the product of the constant terms, so (1) $\Rightarrow$ (2). We claim that (2) $\Rightarrow$ (1). If b_0 is invertible then the equation $b(x)c(x) = 1$ may be solved inductively for $c(x) = \sum_{i=0}^{\infty} c_i x^i$ because $c_0 = b_0^{-1}$ and

$$c_i = -b_0^{-1} \left(b_1 c_{i-1} + b_2 c_{i-1} + \cdots + b_i c_0 \right). \qquad \square$$

The set of polynomials over R is the subring of $R[[x]]$ consisting of those power series with finitely many nonzero coefficients. In fact there is a chain of subrings,

$$\begin{array}{ccccccccccc} R & \subset & R[x] & \subset & E & \subset & R_0(x) & \subset & R[[x]] & \subset & R((x)) \\ & & & & & & \cap & & & & \\ & & & & & & R(x) & & & & \end{array}$$

which is described in the next few sections. The ring $R((x))$ of *formal Laurent series* consists of infinite sums

$$a(x) = a_{-m} x^{-m} + a_{-m+1} x^{-m+1} + \cdots + a_0 + a_1 x + \cdots$$

with coefficients $a_i \in R$ and at most finitely many nonzero terms of negative degree. Addition and multiplication are defined as with power series. The ring of *rational functions* $R(x)$ consists of all fractions $f(x)/g(x)$ where $f, g \in R[x]$ and g is not a zero divisor. So $R(x) = S_1^{-1} R[x]$ is the full ring of fractions, obtained by inverting the set $S_1 \subset R[x]$ consisting of all nonzero-divisors, cf. Section 1.2.h. (The ring $R(x)$ is usually of interest only when R is a field, in which case $S_1 = R[x] - \{0\}$ consists of the nonzero polynomials, cf. Section 4.2.d.) The rings $R_0(x)$ and E merit special attention.

4.2.b Recurrent sequences and the ring $R_0(x)$ of fractions

Let $S_0 \subset R[x]$ denote the multiplicative subset consisting of all polynomials $b(x)$ such that the constant term $b_0 = b(0) \in R$ is invertible in R and define (cf. Section 1.2.h)

$$R_0(x) = S_0^{-1} R[x]$$

to be the ring of fractions $a(x)/b(x)$ with $b(x) \in S_0$. We obtain an injective homomorphism $\psi : R_0(x) \to R[[x]]$ by mapping $a(x)/b(x)$ to the product $a(x)c(x)$ where $c(x) \in R[[x]]$ is the power series inverse of $b(x)$ which was constructed in Lemma 4.2.2. The series

$$\psi(a(x)/b(x)) = a_0 + a_1 x + a_2 x^2 + \cdots \in R[[x]]$$

is referred to as the *power series expansion* of the fraction $a(x)/b(x)$, and we write

$$\mathbf{a} = \mathbf{seq}(a(x)/b(x)).$$

Henceforth we identify $R_0(x)$ with its image in $R[[x]]$.

A sequence $\mathbf{a} = a_0, a_1, \cdots$ of elements of R is *linearly recurrent* (of degree d) if there exist $q_1, \cdots, q_d \in R$ (with $q_1 \neq 0, q_d \neq 0$) such that for all $n \geq d$ we have

$$a_n = q_1 a_{n-1} + \cdots + q_d a_{n-d}. \tag{4.2}$$

More generally, we say that $\mathbf{a}$ satisfies a recurrence of degree d for $n \geq N$ if equation (4.2) holds for all $n \geq N$. The following theorem characterizes the ring $R_0(x)$ as consisting of those power series $a(x)$ having linearly recurrent coefficient sequences.

Theorem 4.2.3. *Let $a = a_0 + a_1 x + \cdots \in R[[x]]$ be a formal power series. Fix $N \geq d > 1$. The following statements are equivalent.*

1. *There exist polynomials $f(x), g(x) \in R[x]$ such that $g(0)$ is invertible, $\deg(g) = d$, $\deg(f) < N$, and $a(x) = f(x)/g(x)$.*
2. *For all $n \geq N$ the sequence of coefficients $a_n, a_{n+1}, a_{n+2}, \cdots = \mathbf{seq}(f/g)$ satisfies a linear recurrence, of degree d.*

Proof. First suppose that statement (1) holds, say $a(x) = f(x)/g(x)$ with $g(x) = g_0 + g_1 x + \cdots + g_d x^d$ and $g_d \neq 0$. Then $f(x) = a(x)g(x)$ which gives

$$f_n = \sum_{i=0}^{d} g_i a_{n-i}$$

for $n \geq d$. Since $f(x)$ is a polynomial, these coefficients vanish for $n > \deg(f)$. Consequently, if $n \geq N \geq \max(d, \deg(f) + 1)$ we have,

$$a_n = -g_0^{-1} \left(g_1 a_{n-1} + g_2 a_{n-2} + \cdots + g_d a_{n-d} \right)$$

which is a linear recurrence (of degree d). Conversely, suppose the coefficients of f satisfy a linear recurrence $a_n = g_1 a_{n-1} + \cdots + g_d a_{n-d}$ (with $g_d \neq 0$) for all $n \geq N$. Let $g(x) = -1 + g_1 x + \cdots + g_d x^d$ and set $g_0 = -1$. Then the product $f(x) = g(x)a(x)$ is a polynomial of degree less than N, because for $n \geq N$ its term of degree n is

$$\sum_{i=0}^{d} g_i a_{n-i} = 0.$$

Consequently $a(x) = f(x)/g(x)$, g_0 is invertible, and $\deg(f) < N$. □

4.2.c Eventually periodic sequences and the ring E

Definition 4.2.4. *The ring $E \subset R[[x]]$ is the collection of all power series $a(x) = \sum_{i=0}^{\infty} a_i x^i$ such that the sequence of coefficients $\mathbf{seq}(a) = (a_0, a_1, \cdots)$ is eventually periodic.*

Theorem 4.2.5. *Let $a(x) = \sum_{i=0}^{\infty} a_i x^i$ be a power series over a ring R and let $n \geq 1$. Then the following are equivalent. (See also Lemma 1.4.6.)*

1. *The sequence $\mathbf{seq}(a) = (a_0, a_1, \cdots)$ is eventually periodic and n is a period of $\mathbf{seq}(a)$.*
2. *$a(x) = h(x)/(x^n - 1)$ for some $h(x) \in R[x]$.*
3. *$a(x) = f(x)/g(x)$ for some $f, g \in R[x]$ such that $g(x)$ is monic and $g(x)|(x^n - 1)$.*
4. *$a(x) = f(x)/g(x)$ for some $f, g \in R[x]$ such that $g(x)|(x^n - 1)$.*

These statements imply

5. *$a(x) = f(x)/g(x)$ for some $f, g \in R[x]$ such that $g(0)$ is invertible in R.*

Hence $E \subseteq R_0(x)$. The eventual period is the least n for which (2), (3), or (4) holds. If R is finite then statement (5) implies the others (for some $n \geq 1$), so $E = R_0(x)$. (In other words, if R is finite then a sequence over R satisfies a linear recurrence if and only if it is eventually periodic.)

The sequence $\mathbf{seq}(a)$ is purely periodic if and only if (2) holds with $\deg(h(x)) < n$ or equivalently, if (3) or (4) holds with $\deg(f(x)) < \deg(g(x))$.

Proof. To see that condition (1) implies condition (2), suppose $a(x)$ is eventually periodic with $a_i = a_{i+n}$ for all $i \geq N$. Then we have

$$\begin{aligned} a(x) &= \sum_{i=0}^{N-1} a_i x^i + x^N \sum_{j=0}^{\infty} \left(\sum_{k=0}^{n-1} a_{nj+i+N} x^i \right) x^{nj} \\ &= \frac{(x^n - 1)(\sum_{i=0}^{N-1} a_i x^i) - x^N \sum_{k=0}^{n-1} a_{nj+i+N} x^i}{x^n - 1}. \end{aligned}$$

This can be written as a rational function with denominator $x^n - 1$.

That conditions (2), (3) and (4) are equivalent is left to the reader. In case (3) or (4), if $b(x)g(x) = x^n - 1$, then $\deg(b(x)f(x)) < n$ if and only if $\deg(f(x)) < \deg(g(x))$, which reduces the statements about purely periodic power series to the statement about purely periodic power series in case (2).

To see that condition (2) implies condition (1), suppose $a(x) = h(x)/(x^n - 1)$ with $h(x) \in R[x]$. By the division theorem we can write $h(x) = (x^n - 1)u(x) + v(x)$ with $u(x), v(x) \in R[x]$ and

$\deg(v(x)) < n$. Thus

$$\begin{aligned} a(x) &= u(x) + \frac{v(x)}{x^n - 1} \\ &= u(x) + (v(x) + x^n v(x) + x^{2n} v(x) + \cdots). \end{aligned}$$

The power series $v(x) + x^n v(x) + x^{2n} v(x) + \cdots$ is strictly periodic since there is no overlap among the degrees of the monomials in any two terms $x^{in} v(x)$ and $x^{jn} v(x)$. The addition of $u(x)$ only affects finitely many terms, so the result is eventually periodic. Also, the sequence is periodic if and only if $u(x) = 0$, which is equivalent to $\deg(h(x)) < n$.

It follows immediately that the eventual period is the least n for which (2), (3), or (4) holds. Lemma 1.4.6 says that (4) implies (5), and if R is finite, then (5) implies (4) (for some n). □

It is not always true that $E = R_0(x)$: take $R = \mathbb{Z}$, $g(x) = 1 - 2x$, and $f(x) = 1$. Then $a(x) = 1 + 2x + 4x^2 + \cdots$ which is not eventually periodic.

4.2.d When R is a field

Theorem 4.2.6. *If R is a field, then $R(x) \subset R((x))$ and both of these are fields. (The former is called the* field of rational functions *over R; it is a* global field*). They are the fraction fields of $R[x]$ and $R[[x]]$ respectively. The only non-trivial ideals in $R[[x]]$ are the principal ideals (x^m) for $m \geq 1$.*

Proof. The only nontrivial statement in this theorem concerns the ideal structure of $R[[x]]$. Suppose that I is a nonzero ideal in $R[[x]]$. Let $a(x)$ be an element of I whose least degree nonzero term has the smallest possible degree, n. Then we have $a(x) = x^n b(x)$ for some $b(x) \in R[[x]]$, and the constant term of $b(x)$ is nonzero. By Lemma 4.2.2, $b(x)$ is invertible in $R[[x]]$. Hence $x^n \in I$. Moreover, every element of I has least degree $\geq n$, so can be written as $x^n c(x)$ for some $c(x) \in R[[x]]$. Hence $I = (x^n)$. □

4.2.e $R[[x]]$ as an inverse limit

The quotient ring $R[x]/(x^i)$ may be (additively, but not multiplicatively) identified with the collection of all polynomials of degree $\leq i - 1$. Let

$$\psi_i : R[[x]] \to R[x]/(x^i)$$

be the homomorphism that associates to each $a = \sum_{i=0}^{\infty} a_i x^i$ the partial sum (that is, the polynomial)

$$\psi_i(a) = a_0 + a_1 x + \cdots + a_{i-1} x^{i-1}.$$

These homomorphisms are compatible in the sense that if $k \leq i$ then

$$\psi_{i,k}(\psi_i(a)) = \psi_k(a)$$

where

$$\psi_{i,k} : R[x]/(x^i) \to R[x]/(x^k)$$

is reduction modulo x^k. The next lemma says that every element of $R[[x]]$ can be described in terms of such a sequence of partial sums.

Lemma 4.2.7. *Suppose $s_1, s_2, \cdots$ is a sequence with $s_i \in R[x]/(x^i)$. Assume these elements are* compatible *in the sense that $\psi_{i,k}(s_i) = s_k$ for every pair $k \leq i$. Then there is a unique element $a \in R[[x]]$ such that $\psi_i(a) = s_i$ for all $i \geq 1$.*

Proof. The element $a = \sum_{i=0}^{\infty} a_i x^i$ is given by $a_i = (\psi_{i+1}(a) - \psi_i(a))/x^i$. □

This lemma implies that $R[[x]] = \varprojlim \{R[x]/(x^i)\}$, is the inverse limit of the system of rings $R[x]/(x^i)$. See Section 1.2.l to recall the definition of inverse limits. Specifically, the set of rings $\{R[x]/(x^i)\}$ is a directed system indexed by the positive integers, with the reduction functions $\psi_{i,k}$. Thus there is a homomorphism ψ from $R[[x]]$ to $\varprojlim \{R[x]/(x^i)\}$ so that if

$$\varphi_i : \varprojlim \{R[x]/(x^i)\} \to R[x]/(x^i)$$

is the projection function, then $\psi_i = \varphi_i \circ \tau$. This is shown in Figure 4.1.

We claim that ψ is an isomorphism. Lemma 4.2.7 says that ψ is surjective. If $a(x) = \sum_{i=0}^{\infty} a_i x^i \in R[[x]]$ is nonzero, then $a_i \neq 0$ for some i. Then $\psi_i(a) \neq 0$, so also $\psi(a) \neq 0$. Thus ψ is also injective, and thus an isomorphism.

Corollary 4.2.8. *Let M be an Abelian group. For $i = 1, 2, \cdots$ let $\tau_i : M \to R[x]/(x^i)$ be group homomorphisms satisfying $\tau_i = \psi_{j,i} \circ \tau_j$ whenever $i \leq j$. Then there is a unique homomorphism $\tau : M \to R[[x]]$ so that $\tau_i = \psi_i \circ \tau$ for $i = 1, 2, \cdots$. If M is also a module over R (respectively, an algebra) and the τ_i are R-module homomorphisms (resp., ring homomorphisms), then so is τ.*

4.3 Reciprocal Laurent series

Let K be a field, let $g(x) \in K[x]$ be a polynomial of degree d. The *reciprocal polynomial* is the polynomial $g^*(y) = y^d g(1/y)$.

It is straightforward to check that $(gh)^* = g^* h^*$ for any $h \in K[x]$, and that $(g^*)^* = g$ if and only if $g(0) \neq 0$. If the polynomial g has nonzero constant term, then it is irreducible (resp. primitive)

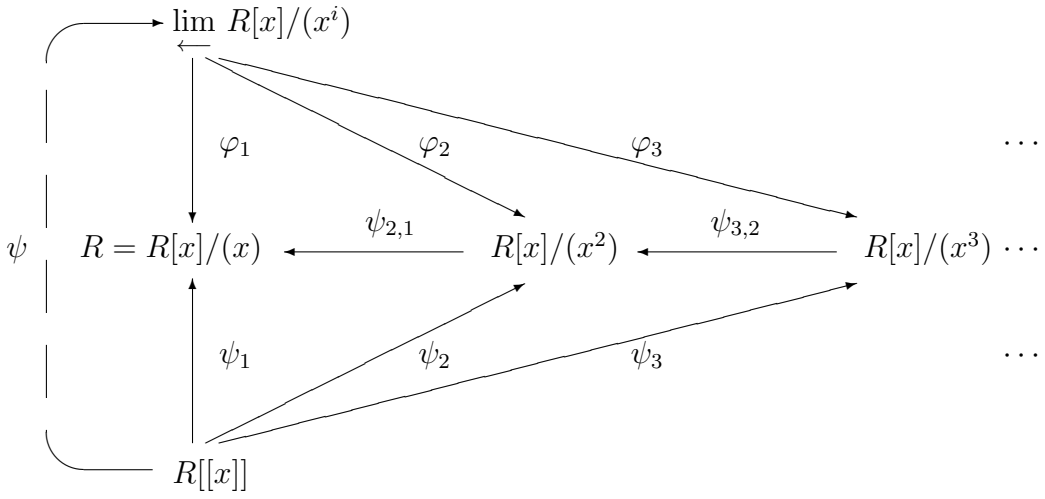


Figure 4.1: $R[[x]]$ as an inverse limit

if and only if the same is true of g^*. If $\alpha \neq 0$ is a root of g (possibly in some extension field of K) then α^{-1} is a root of g^*. Let

$$F = K((x^{-1})) = \left\{ \sum_{i=k}^{\infty} a_i x^{-i} : k \in \mathbb{Z}, a_i \in K \right\}$$

be the ring of formal Laurent series in x^{-1}. According to Theorem 4.2.6, F is a field. Every polynomial $f(x) \in K[x]$ is in F. Therefore F also contains every rational function $f(x)/g(x)$ (where $f, g \in K[x]$). Such a function can therefore be expanded as a Laurent series in x^{-1}. Some of these will be a power series in x^{-1}. It is sometimes helpful, by analogy with the real numbers, to think of $\sum_{i=k}^{0} a_i x^{-i}$ as the integer part of $a = \sum_{i=k}^{\infty} a_i x^{-i}$, and to think of $\sum_{i=1}^{\infty} a_i x^{-i}$ as the fractional part. The degree of a is $-k$ if $a_k \neq 0$.

Proposition 4.3.1. *Let $f, g \in K[x]$ be polynomials. Then $\deg(f) \leq \deg(g)$ if and only if the rational function $f(x)/g(x)$ is actually a power series in x^{-1}, that is,*

$$\frac{f(x)}{g(x)} = a_0 + a_1 x^{-1} + a_2 x^{-2} + \cdots \in K[[x^{-1}]], \tag{4.3}$$

and $\deg(f) < \deg(g)$ if and only if $a_0 = 0$. The sequence $\mathbf{a} = a_0, a_1, a_2, \cdots$ satisfies a linear recurrence with connection polynomial g^*. Conversely, any element of $K[[x^{-1}]]$ whose coefficients

satisfy a linear recurrence with connection polynomial g^* may be expressed as a rational function as in equation (4.3). The sequence **a** *is eventually periodic if and only if there exists N so that $g(x)|(x^N-1)$ (which always holds if K is a finite field). The sequence* **a** *is strictly periodic if and only if it is eventually periodic and $f(0)=0$ (meaning that $f(x)$ is divisible by x).*

Proof. Let $a(x)=a_0+a_1x^{-1}+\cdots$, let $f(x)=f_0+f_1x+\cdots+f_rx^r$ and $g(x)=g_0+g_1x+\cdots+g_dx^d$. If equation (4.3) holds then $g(x)a(x)=f(x)$ is a polynomial of degree $r=\deg(g)+\deg(a)\le d$, whose degree d term is $f_d=g_da_0$, which vanishes when $a_0=0$. The absence of negative powers of x in $f(x)$ exactly says that the sequence **a** satisfies a linear recurrence with connection polynomial g^*. Next, suppose the sequence **a** is eventually periodic. Then there exists N such that $g^*(y)|(y^N-1)$, from which it follows that $g(x)|(x^N-1)$ (and vice versa). Finally, let $\widehat{f}(y)=y^df(1/y)=f_0y^d+f_1y^{d-1}+\cdots+f_ry^{d-r}$ so that

$$\frac{\widehat{f}(y)}{g^*(y)}=\frac{f(1/y)}{g(1/y)}=a_0+a_1y+a_2y^2+\cdots.$$

The sequence **a** is strictly periodic when $\deg(\widehat{f})<\deg(g^*)=d$, i.e., when $f_0=0$. □

4.4 N-Adic numbers

4.4.a Definitions

The p-adic numbers were discovered by K. Hensel around 1900. He was pursuing the idea that numbers were like functions – the p-ary expansion of an integer is like a polynomial, so what number corresponds to a power series? His ideas led to many far-reaching discoveries that have shaped much of the modern approach to number theory. Fix an integer $N\ge 2$.

Definition 4.4.1. *An* N-adic integer *is an infinite expression*

$$a=a_0+a_1N+a_2N^2+\cdots, \tag{4.4}$$

where $a_0,a_1,\cdots\in\{0,1,\cdots,N-1\}$. The set of N-adic integers is denoted by $\mathbb{Z}_N$. The least degree *of a nonzero N-adic integer $a=\sum_{i=0}^{\infty}a_iN^i$ is the least index i such that $a_i\neq 0$. The least degree of 0 is ∞.*

The a_i are called *coefficients*.When writing N-adic integers we may omit terms whose coefficients are zero. We may also write the terms in a different order. A series such as equation (4.4) does not converge in the usual sense. Nevertheless it can be manipulated as a formal object, just

as with power series, but with slightly different algebraic rules. Addition and multiplication are defined so as to take into account the "carry" operation. To be precise, the statement

$$\sum_{i=0}^{\infty} a_i N^i + \sum_{i=0}^{\infty} b_i N^i = \sum_{i=0}^{\infty} c_i N^i \tag{4.5}$$

with $a_i, b_i, c_i \in \{0, 1, \cdots, N-1\}$ means that there exist integers $t_0, t_1, \cdots \in \{0, 1\}$ so that

$$a_0 + b_0 = c_0 + N t_0 \tag{4.6}$$

and for all $i \geq 1$,

$$a_i + b_i + t_{i-1} = c_i + N t_i. \tag{4.7}$$

The quantity t_i is called the *carry* and it is 0 or 1 since (by induction) $a_i + b_i + t_{i-1} \leq 2(N-1)+1 < 2N$. Also by induction the numbers t_i, c_i are determined by the a_k, b_k. In fact,

$$c_n = (a_n + b_n + t_{n-1}) \pmod{N} \quad \text{and} \quad t_n = \lfloor (a_n + b_n + t_{n-1})/N \rfloor$$

(with $t_{-1} = 0$). The product $ab = c$ is defined similarly with

$$\sum_{i=0}^{n} a_i b_{n-i} + t_{n-1} = c_n + N t_n, \tag{4.8}$$

although in this case the carry t_i may be greater than 1. (Some readers may find it easier to think in terms of power series in some indeterminate, say, Y, and to use the rule that $NY^i = Y^i + Y^i + \cdots + Y^i = Y^{i+1}$. But this notation quickly becomes cumbersome. The use of N instead of Y facilitates many computations.)

It is easy to see that these operations make $\mathbb{Z}_N$ into a ring (the ring axioms hold in $\mathbb{Z}_N$ because they hold modulo N^k for every k). As with power series, we refer to the sequence $(a_0, a_1, \cdots)$ of coefficients as $\mathbf{seq}_N(a)$. It is an N-ary sequence (that is, a sequence over the alphabet $\{0, 1, \cdots, N-1\}$). We say that a is periodic (resp. eventually periodic) if the sequence $\mathbf{seq}_N(a)$ of coefficients is periodic (resp. eventually periodic).

If $a = \sum_{i=0}^{\infty} a_i N^i$ is an N-adic integer, then the coefficient a_0 is called the *reduction of a modulo* N and it is denoted $a_0 = a \pmod{N}$. This gives a ring homomorphism $\mathbb{Z}_N \to \mathbb{Z}/(N)$. We also define the *integral quotient* of a by N to be

$$a \text{ (div } N) = \sum_{i=0}^{\infty} a_{i+1} N^i = \frac{a - a_0}{N}.$$

Thus $a = a \pmod{N} + N(a \text{ (div } N))$.

In the ring $\mathbb{Z}_N$ we have an identity, $-1 = (N-1) + (N-1)N + (N-1)N^2 + \cdots$, which can be verified by adding 1 to both sides. Similarly, there is an explicit formula for multiplication by -1. If $a = \sum_{i=d}^{\infty} a_i N^i$ with $1 \le a_d \le N-1$, then

$$-a = (N - a_d)N^d + \sum_{i=1}^{\infty} (N - a_i - 1)N^i. \tag{4.9}$$

It follows that $\mathbb{Z}_N$ contains the integers as a subring, and in fact there is a chain of rings, similar to that of Section 4.2.a,

$$\begin{array}{ccccccc} \mathbb{Z} & \subset & \mathbb{Z}_{N,0} & \subset & \mathbb{Z}_N & \subset & \mathbb{Q}_N \\ & & \cap & & & & \\ & & \mathbb{Q} & & & & \end{array}$$

The following analog to Lemma 4.2.2 characterizes the invertible elements of $\mathbb{Z}_N$.

Lemma 4.4.2. *Let $a = \sum_{i=0}^{\infty} a_i N^i \in \mathbb{Z}_N$. Then a is invertible in $\mathbb{Z}_N$ if and only if a_0 is relatively prime to N.*

Proof. The proof is essentially the same as that of Lemma 4.2.2. Recall from Section 1.2.d that $a_0 \in \mathbb{Z}$ is relatively prime to N if and only if a_0 is invertible in $\mathbb{Z}/(N)$. We want to find $b = \sum_{i=0}^{\infty} b_i N^i$ so that $ab = 1$, and $0 \le b_i \le N-1$. By equation (4.8) this means $a_0 b_0 = 1 + N t_0$ (which has the unique solution $b_0 = a_0^{-1} \pmod N$ and $t_0 = a_0 b_0 - 1 \text{ (div } N)$) and

$$\sum_{i=0}^{n} a_i b_{n-i} + t_{n-1} = c_n + N t_n,$$

which has the unique solution recursively given by

$$\begin{aligned} b_n &= a_0^{-1} \left(c_n - t_{n-1} - \sum_{i=1}^{n} a_i b_{n-i} \right) \pmod N \\ t_n &= \left(\sum_{i=0}^{n} a_i b_{n-i} - c_n \right) \text{ (div } N). \end{aligned}$$

□

4.4.b The ring $\mathbb{Q}_N$

The ring $\mathbb{Q}_N$ of *N-adic numbers* is the analog of formal Laurent series; it consists of infinite sums

$$a(x) = a_{-m} N^{-m} + a_{-m+1} N^{-m+1} + \cdots + a_0 + a_1 N + \cdots$$

with coefficients $0 \le a_i \le N-1$ and at most finitely many nonzero terms of negative degree. Addition and multiplication are defined as with N-adic integers. We have $\mathbb{Q}_N = S^{-1}\mathbb{Z}_N$ where $S = \{N, N^2, N^3 \cdots\}$.

It follows from Lemma 4.4.2 that if $N = p$ is a prime number, then $\mathbb{Z}_p$ is an integral domain and $\mathbb{Q}_p$ is its fraction field, that is, $\mathbb{Q}_p = S^{-1}\mathbb{Z}_p$ where $S = \mathbb{Z}_p^\times$ consists of all nonzero elements (cf. Section 1.2.h). For composite N, the ring $\mathbb{Z}_N$ has zero divisors and the ring $\mathbb{Q}_N$ is not a field. However in Corollary 4.4.9 we show that $\mathbb{Q}_N = S^{-1}\mathbb{Z}_N$ is the "full" ring of fractions, meaning that the set S consists of all nonzero-divisors in $\mathbb{Z}_N$. In Theorem 4.4.8 we show that $\mathbb{Z}_N$ and $\mathbb{Q}_N$ can be described in terms of $\mathbb{Z}_p$ and $\mathbb{Q}_p$ as p ranges over the prime divisors of N. For these reasons, the rings $\mathbb{Z}_N$ and $\mathbb{Q}_N$ (with N composite) are seldom encountered in the mathematical literature. However we make use of them when studying sequences generated by an FCSR.

4.4.c The ring $\mathbb{Z}_{N,0}$

Definition 4.4.3. *The ring $\mathbb{Z}_{N,0}$ consists of the set of all rational numbers $a/b \in \mathbb{Q}$ (in lowest terms) such that b is relatively prime to N. That is, $\mathbb{Z}_{N,0} = S^{-1}\mathbb{Z}$, where S is the multiplicative set $\{b \in \mathbb{Z} : \gcd(b, N) = 1\}$.*

Lemma 4.4.2 says that $\mathbb{Z}_{N,0}$ is naturally contained in the N-adic integers $\mathbb{Z}_N$ and it is a subring. The next theorem identifies $\mathbb{Z}_{N,0}$ as the collection of N-adic integers $a \in \mathbb{Z}_N$ such that $\mathbf{seq}_N(a)$ is eventually periodic.

Theorem 4.4.4. *Let $a = \sum_{i=0}^{\infty} a_i N^i \in \mathbb{Z}_N$ and let $n \ge 1$. Then the following statements are equivalent.*

1. *$a = f/g$ for some $f, g \in \mathbb{Z}$ such that $g > 0$ is relatively prime to N and $\mathrm{ord}_g(N)$ divides n.*
2. *$a = f/g$ for some $f, g \in \mathbb{Z}$ such that $g > 0$ and $g|(N^n - 1)$.*
3. *$a = h/(N^n - 1)$ for some $h \in \mathbb{Z}$.*
4. *$\mathbf{seq}_N(a)$ is eventually periodic and n is a period of a.*

The eventual period is the least n for which (1), (2) or (3) holds. The N-adic integer a is purely periodic if and only if $-(N^n - 1) \le h \le 0$ in case (3) or $-g \le f \le 0$ in cases (1) and (2).

Proof. Recall from Section 1.2.d that the integer g is relatively prime to N if and only if there exists $n \ge 0$ so that $g|(N^n - 1)$, and the smallest such is $n = \mathrm{ord}_g(N)$. (See also Lemma 1.4.6.) Hence (1) and (2) are equivalent. That (2) and (3) are equivalent is left to the reader.

To see that (4) implies (3) let us first consider the special case when a is strictly periodic with period n. Set $h = a_0 + a_1 N + \cdots + a_{n-1}N^{n-1}$. Then $0 \le h \le N^n - 1$ and

$$a = h(1 + N^n + N^{2n} + \cdots) = h/(1 - N^n) = -h/(N^n - 1) \tag{4.10}$$

as claimed. (Notice that no carries occur in the above product.) If a is eventually periodic, suppose it becomes periodic after the mth term. Then we can write $a = H + N^m b$ for some integer $H \geq 0$, where $b \in \mathbb{Z}_N$ is strictly periodic. Applying the special case to b and taking a common denominator gives $a = h'/(N^n - 1)$ for some $h' \in \mathbb{Z}$.

To see that (3) implies (4), let us first consider the special case when $1 - N^n \leq h \leq 0$. Then $0 \leq -h \leq N^n - 1$ so $-h$ can be uniquely expressed as a sum, $-h = a_0 + a_1 N + \cdots + a_{n-1} N^{n-1}$ with $0 \leq a_i < N$. Consequently equation (4.10) holds and since there are no carries in the product that occurs there, the sequence $\mathbf{seq}_N(a)$ is strictly periodic.

Now we show how to reduce to the case that $1 - N^n < h \leq 0$. If $h > 0$ then $-h < 0$ and according to equation (4.9), multiplication by -1 does not affect the eventual periodicity (nor the eventual period) of an N-adic number. So we may assume $h \leq 0$. If $h \leq 1 - N^n < 0$ then we can write $a = H + h'/(N^n - 1)$ where $H \in \mathbb{Z}$, $H < 0$, and $1 - N^n < h' \leq 0$. Therefore $-a = (-H) + (-h')/(N^n - 1)$ is eventually periodic because the addition of the positive integer $-H$ to the eventually periodic expansion of $(-h')/(N^n - 1)$ still leaves an eventually periodic series. Using equation (4.9) again, it follows that the N-adic expansion of a is also eventually periodic.

It follows immediately that the eventual period is the least n for which (1), (2) or (3) holds. □

Corollary 4.4.5. *Let $f, g, \in \mathbb{Z}$ with $\gcd(g, N) = 1$. If $\gcd(f, g) = 1$, then the period of the N-adic expansion $\mathbf{seq}_N(f/g)$ is the multiplicative order of N modulo g.*

4.4.d $\mathbb{Z}_N$ as an inverse limit

Let $\psi_\ell : \mathbb{Z}_N \to \mathbb{Z}/(N^\ell)$ be the homomorphism that associates to each $a = \sum_{i=0}^{\infty} a_i N^i$ the partial sum

$$\psi_\ell(a) = \sum_{i=0}^{\ell-1} a_i N^i.$$

These homomorphisms are compatible in the sense that if $k \leq \ell$ then

$$\psi_{\ell,k}(\psi_\ell(a)) = \psi_k(a)$$

where

$$\psi_{\ell,k} : \mathbb{Z}/(N^\ell) \to \mathbb{Z}/(N^k)$$

is reduction modulo N^k. In the language of Section 1.2.l, the family of rings $\mathbb{Z}/(N^\ell)$ is a directed system indexed by the positive integers with the maps $\psi_{\ell,k}$. The next lemma says that every N-adic integer can be described as such a sequence of partial sums. It is an exact parallel of Lemma 4.2.7.

Lemma 4.4.6. *For all $N > 1$, the mappings $\psi_{\ell,k}$ induce an isomorphism of rings,*

$$\mathbb{Z}_N \cong \varprojlim \{\mathbb{Z}/(N^i)\}.$$

In other words, there is a one to one correspondence between $\mathbb{Z}_N$ and the set of all sequences $(s_0, s_1, \cdots)$ with $s_i \in \mathbb{Z}/(N^i)$ such that for all pairs $i \leq j$ we have $\psi_{j,i}(s_j) = s_i$.

Proof. By Theorem 1.2.33 there is a unique induced map $\psi : \mathbb{Z}_N \to \varprojlim \{\mathbb{Z}/(N^i)\}$. It suffices to construct an inverse for this function. Suppose $s = (s_1, s_2, \cdots) \in \varprojlim \{\mathbb{Z}/(N^i)\}$. That is, $s_i \in \mathbb{Z}/(N^i)$ and for all pairs $i \leq j$ we have $\psi_{j,i}(s_j) = s_i$. Let a_i be the coefficient of N^i in the N-adic expansion of s_{i+1}. By the commutativity assumptions, this is also the coefficient of N^i in s_j for all $j > i$. Define $\tau(s) = \sum_{i=0}^{\infty} a_i N^i \in \mathbb{Z}_N$. Then $\psi(\tau(s)) = s$, so τ is the desired inverse. This is illustrated in Figure 4.2. □

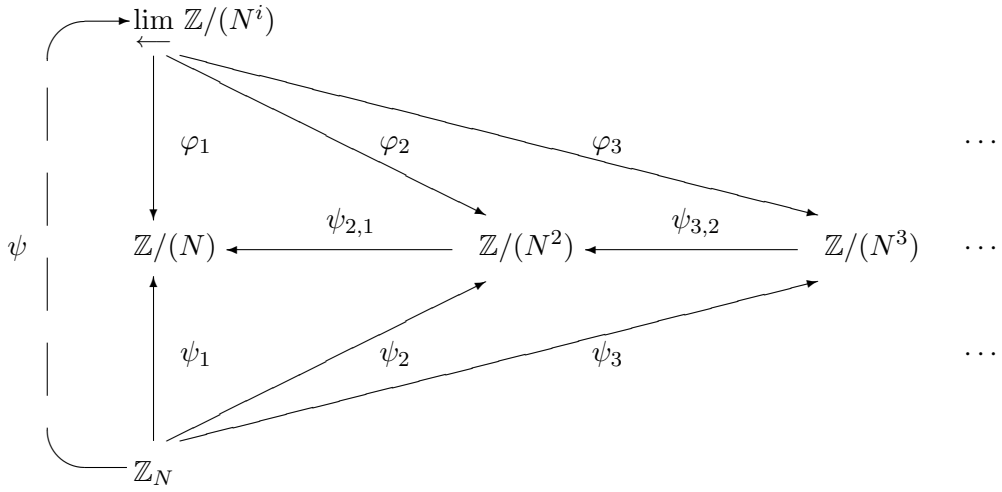


Figure 4.2: $\mathbb{Z}_N$ as an inverse limit

Corollary 4.4.7. *Let M be an Abelian group. For $i = 1, 2, \cdots$ let $\tau_i : M \to \mathbb{Z}/(N^i)$ be group homomorphisms satisfying $\tau_i = \psi_{j,i} \circ \tau_j$ whenever $i \leq j$. Then there is a unique homomorphism $\tau : M \to \mathbb{Z}_N$ so that $\tau_i = \psi_i \circ \tau$ for $i = 1, 2, \cdots$. If M is also a ring and the τ_i are homomorphisms, then so is τ.*

4.4.e Structure of $\mathbb{Z}_N$

In this section we suppose the prime factorization of N is $N = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}$, with distinct primes p_i. The ring $\mathbb{Z}_N$ can be expressed in terms of the p-adic integers $\mathbb{Z}_{p_i}$.

Theorem 4.4.8. *With N as above, the ring $\mathbb{Z}_N$ is isomorphic to the ring $\mathbb{Z}_{p_1} \times \mathbb{Z}_{p_2} \times \cdots \times \mathbb{Z}_{p_k}$. Similarly, $\mathbb{Q}_N \cong \mathbb{Q}_{p_1} \times \cdots \times \mathbb{Q}_{p_k}$.*

Proof. To simplify the notation slightly set $q_i = p_i^{n_i}$. For each j and ℓ, we have a homomorphism from $\mathbb{Z}/(N^\ell)$ to $\mathbb{Z}/(q_i^\ell)$. This induces a homomorphism from $\mathbb{Z}_N$ to $\mathbb{Z}/(q_i^\ell)$, and all the appropriate functions commute. Thus by the universal property of inverse limits, there are homomorphisms

$$\gamma_i : \mathbb{Z}_N \to \mathbb{Z}_{q_i}$$

with appropriate commutativity. This gives us a homomorphism

$$\gamma : \mathbb{Z}_N \to \prod_{i=1}^{k} \mathbb{Z}_{q_i},$$

which we now show to be an isomorphism by constructing an inverse. For every positive ℓ there is a reduction homomorphism

$$\delta_\ell : \prod_{i=1}^{k} \mathbb{Z}_{q_i} \to \prod_{i=1}^{k} \mathbb{Z}/(q_i^\ell).$$

By the Chinese Remainder Theorem (Theorem 1.2.18), the latter ring is isomorphic to $\mathbb{Z}/(N^\ell)$. Everything commutes appropriately, so there is an induced map

$$\delta : \prod_{i=1}^{k} \mathbb{Z}_{q_i} \to \mathbb{Z}_N.$$

It is straightforward to see that γ and δ are inverses (it follows, for example, from the uniqueness of the induced map into the universal object $\mathbb{Z}_N$).

This reduces the theorem to the case where $N = p^n$ for some prime p. Let

$$a = \sum_{i=0}^{\infty} a_i p^{ni} \in \mathbb{Z}_{p^n}, \tag{4.11}$$

with $0 \le a_i < p^n$. Each coefficient can be uniquely expressed as $a_i = \sum_{j=0}^{n-1} a_{i,j} p^j$ with $0 \le a_{i,j} < p$. Substituting this into (4.11) gives a p-adic integer. It is straightforward to verify that the resulting mapping $\mathbb{Z}_{p^n} \to \mathbb{Z}_p$ is a ring isomorphism.

The ring $\mathbb{Q}_N$ is obtained from $\mathbb{Z}_N$ by inverting N, which is equivalent to inverting $p_1, p_2, \cdots, p_k$ simultaneously. It follows that $\mathbb{Q}_N \cong \prod_{i=1}^{k} \mathbb{Q}_{p_i}$. □

Corollary 4.4.9. *The ring $\mathbb{Q}_N = S^{-1}\mathbb{Z}_N$ is obtained by inverting the set S consisting of all non-zero-divisors in $\mathbb{Z}_N$. The ring $\mathbb{Z}_N$ has no zero divisors if and only if N is prime.*

Proof. Use the isomorphism $\mathbb{Z}_N \cong \prod_{i=1}^k \mathbb{Z}_{p_i}$ of Theorem 4.4.8. Then an element $a = (a_1, a_2, \cdots, a_k)$ in this product is a zero divisor if and only if at least one of the coordinates $a_j = 0$ (since then, if b has a 1 in the jth position and zeroes elsewhere, we have $ab = 0$). So the set S of non-zero-divisors consists of all such k-tuples where all of the a_j are nonzero. Hence, $S = S_1 \times S_2 \times \cdots \times S_k$ is the product of the sets $S_i = \mathbb{Z}_{p_i}^\times$ of nonzero elements in $\mathbb{Z}_{p_i}$. So inverting this set gives $\prod_{i=1}^k \mathbb{Q}_{p_i} \cong \mathbb{Q}_N$. □

There are many irrational algebraic numbers in $\mathbb{Z}_N$. For example, suppose that $u(x)$ is a polynomial with integer coefficients that has a root modulo N. Then $u(x)$ has a root in $\mathbb{Z}_N$. This is proved in the next section using Hensel's Lemma.

4.5 π-Adic numbers

In this section we put the constructions from Subsections 4.2 and 4.4 into a larger context that enables us to build very general algebraic sequence generators. Let R be an integral domain. Let $\pi \in R$.

In the case of power series, we took coefficients from the underlying ring. In the case of N-adic integers we took coefficients from $\{0, 1, \cdots, N-1\}$. When we construct π-adic numbers, the generalizations of power series and N-adic integers, there may be no such natural set to use for coefficients so we take a slightly different approach.

4.5.a Construction of R_π

Definition 4.5.1. *A* pre-π-adic number over R *is an infinite expression*

$$a = a_0 + a_1\pi + a_2\pi^2 + \cdots,$$

with $a_0, a_1, \cdots \in R$. Let $\widehat{R}_\pi$ denote the set of pre-π-adic numbers.

The a_i are the *coefficients*, and the sequence $(a_0, a_1, \cdots)$ is referred to as $\mathbf{seq}(a)$ or $\mathbf{seq}_\pi(a)$. When writing pre-π-adic numbers we may omit terms whose coefficient is zero. We may also write the terms in a different order. The coefficients are arbitrary and may even be multiples of π. In fact a pre-π-adic number is just a power series over R, so $\widehat{R}_\pi$ is a commutative ring.

We want to think of certain pre-π-adic numbers as representing the same element. For example, $\pi \cdot 1 + 0 \cdot \pi + 0 \cdot \pi^2 \cdots$ and $0 \cdot 1 + 1 \cdot \pi + 0 \cdot \pi^2 \cdots$ should be equal. We accomplish this by taking a

quotient by an appropriate ideal. For each positive integer n we have a function $\widehat{\varphi}_n : \widehat{R}_\pi \to R/(\pi^n)$ defined by discarding terms of degree $\geq n$ and mapping the resulting element of R to $R/(\pi^n)$,

$$\widehat{\varphi}_n(\sum_{i=0}^{\infty} a_i\pi^i) = \sum_{i=0}^{n-1} a_i\pi^i \pmod{\pi^n}.$$

Let $I = \bigcap_{n=1}^{\infty} \mathrm{Ker}(\widehat{\varphi}_\mathrm{n})$. (This ideal contains many nonzero elements; see Exercise 9.)

Definition 4.5.2. *The ring of* π-adic integers over R *is the quotient ring* $R_\pi = \widehat{R}_\pi/I$.

If the context is clear we may simply refer to a π-adic integer. The homomorphism $h : R \to R_\pi$ (given by $a \mapsto a\pi^0 + 0 + 0\cdots$) is injective if and only if

$$\bigcap_{i=0}^{\infty}(\pi^i) = (0). \tag{4.12}$$

because its kernel is the set of $a \in R$ such that $\pi^n | a$ for all n. In studying sequences we often focus on rings that satisfy equation (4.12) since we can replace R by $R/\cap_{i=0}^{\infty}(\pi^i)$ without changing R_π.

The element π generates an ideal in R_π, and the homomorphism $h : R \to R_\pi$ induces an isomorphism $R/(\pi^n) \cong R_\pi/(\pi^n)$ for all n. (First check that h induces an injection from $R/(\pi^n)$ to $R_\pi/(\pi^n)$. But any $a = \sum_{i=0}^{\infty} a_i\pi^i \in R_\pi/(\pi^n)$ is the image of $\sum_{i=0}^{n-1} a_i\pi^i \in R/(\pi^n)$, so it is also a surjection.)

A more convenient way of representing π-adic integers is the following. By a *complete set of representatives for* R *modulo* π we mean a set S such that for all $a \in R$ there is a unique $b \in S$ so that $a \equiv b \pmod{\pi}$. The set S is not necessarily closed under addition or multiplication, however it often happens that additively or multiplicatively closed sets S can be found.

Theorem 4.5.3. *Let* R *be an integral domain, let* $\pi \in R$ *and let* S *be a complete set of representatives for* R *modulo* π. *Then every* π*-adic integer* $a \in R_\pi$ *has a unique* π*-adic expansion* $a = \sum_{i=0}^{\infty} b_i\pi^i$ *with all* $b_i \in S$.

Proof. Let $a = \sum_{i=0}^{\infty} a_i\pi^i \in R_\pi$. We need to construct a sequence $b_0, b_1, \cdots \in S$ so that for all n

$$\pi^n | \sum_{i=0}^{n-1}(a_i - b_i)\pi^i, \tag{4.13}$$

for then equation (4.12) will imply that $a = \sum b_i\pi^i$. Let $b_0 \in S$ be the unique element so that $a_0 \equiv b_0 \pmod{\pi}$. Inductively assume that we have found $b_0, \cdots, b_{n-1}$ so that equation (4.13) holds. Then

$$\sum_{i=0}^{n-1}(a_i - b_i)\pi^i = \pi^n c$$

for some $c \in R$. Let b_n be the unique element of S such that π divides $a_n - b_n + c$. There is a $d \in R$ such that $a_n + c = b_n + \pi d$. Then

$$\begin{aligned}\sum_{i=0}^{n}(a_i - b_i)\pi^i &= (a_n - b_n)\pi^n + \sum_{i=0}^{n-1}(a_i - b_i)\pi^i \\ &= (a_n - b_n)\pi^n + c\pi^n \\ &= d\pi^{n+1}.\end{aligned}$$

This proves the existence part of the theorem.

Suppose $c_0, c_1, \cdots \in S$ is a second set of coefficients such that

$$\pi^n \left| \sum_{i=0}^{n-1}(a_i - c_i)\pi^i \right.$$

for all n. Then also

$$\pi^n \left| \sum_{i=0}^{n-1}(b_i - c_i)\pi^i \right.$$

for all n. Then $\pi|(b_0 - c_0)$ which implies $b_0 = c_0$. Inductively suppose that $b_i = c_i$ for $i < n$. Then

$$\pi^{n+1} \,|(b_n - c_n)\pi^n.$$

But R is an integral domain, so $\pi|(b_n - c_n)$, so $b_n = c_n$. □

For example, the power series ring $A[[x]]$ over a ring A is the ring R_π where $R = A[x]$ and $\pi = x$, so it is the ring of x-adic integers over $A[x]$, in the terminology of this section. Also, the ring $\mathbb{Z}_N$ of N-adic integers (in the terminology of the preceding section) is the ring R_π where $R = \mathbb{Z}$ and $\pi = N$, so it is the ring of N-adic integers over $\mathbb{Z}$.

4.5.b Divisibility in R_π

Relative to a fixed complete set of representatives S for R modulo π, there is a well defined notion of the reduction of an element of R_π modulo π in R, and of the integral quotient of an element of R_π by π. If

$$a = \sum_{i=0}^{\infty} a_i \pi^i,$$

is a π-adic integer with $a_0, a_1 \cdots \in S$, then we write $a_0 = a \pmod{\pi}$ and refer to it as the *reduction of a modulo π*. The *integral quotient* of a by π is

$$a \ (\mathrm{div}_S \ \pi) = \sum_{i=0}^{\infty} a_{i+1}\pi^i = (a - a_0)/\pi.$$

If $a \in R$, then $a\ (\mathrm{div}_S\ \pi) \in R$ also. If the set S is understood, we simply write $a\ (\mathrm{div}\ \pi)$. Thus in general $a = a\ \pmod{\pi} + \pi(a\ (\mathrm{div}\ \pi))$.

Recall from Section 1.2.e that $q, \pi \in R$ are *relatively prime* if the following equivalent conditions hold.

- $(q) + (\pi) = R$
- The image of q in $R/(\pi)$ is invertible.
- The image of π in $R/(q)$ is invertible.

Proposition 4.5.4. *Let R be an integral domain with fraction field F. Let $\pi \in R$ and assume equation (4.12) holds. Then an element $q \in R$ is invertible in R_π if and only if q and π are coprime. Thus $R_\pi \cap F$ consists of all fractions u/q such that q, π are coprime.*

Proof. If q is invertible in R_π then there exists $u \in R_\pi$ so that $qu = 1$. Reducing this equation modulo π implies that q is invertible in $R_\pi/(\pi) \cong R/(\pi)$ so q and π are coprime. To verify the converse, let $S \subset R$ be a complete set of representatives for $R/(\pi)$ and let $q = \sum_{i=0}^{\infty} q_i \pi^i$ with $q_i \in S$. By hypothesis, q_0 is invertible in $R/(\pi)$. We seek $u = \sum_{i=0}^{\infty}$ with $u_i \in S$ such that $qu = 1$, which is to say that $q_0 u_0 \equiv 1\ \pmod{\pi}$ and, for all $n \geq 1$,

$$q_0 u_n + q_1 u_{n-1} + \cdots + q_n u_0 \equiv 0\ \pmod{\pi}.$$

These equations may be solved recursively for u_n, using the fact that q_0 is invertible in $R/(\pi)$. □

4.5.c The example of $\pi^d = N$

Fix integers $N, d > 0$ such that the polynomial $x^d - N$ is irreducible over the rational numbers $\mathbb{Q}$. This occurs precisely when (1) for any prime number k dividing d, the integer N is not a kth power of an integer, and (2) if 4 divides d, then N is not of the form $-4x^2$ where x is an integer; see [20, p. 221]. Let $\pi \in \mathbb{C}$ be a fixed root of this polynomial; it can be chosen to be a positive real number. The ring $R = \mathbb{Z}[\pi]$ consists of all polynomials in π, with integer coefficients. It is an integral domain in which every prime ideal is maximal.

We claim that the set $S = \{0, 1, \cdots, N-1\} \subset R = \mathbb{Z}[\pi]$ is a complete set of representatives for the quotient $R/(\pi)$. The mapping $\mathbb{Z}[\pi] \to \mathbb{Z}[\pi]/(\pi)$ throws away all the terms of degree ≥ 1 in any polynomial $u \in \mathbb{Z}[\pi]$. Consequently the composition $\mathbb{Z} \to R = \mathbb{Z}[\pi] \to R/(\pi)$ is surjective. So it suffices to show that $R/(\pi)$ contains N elements. In fact the ring $\mathbb{Z}[\pi]$ is an order (but not necessarily the maximal order) in its fraction field $F = \mathbb{Q}(\pi)$ so Lemma 2.4.8 gives:

$$|R/(\pi)| = \left|\mathsf{N}_{\mathbb{Q}}^{F}(\pi)\right|,$$

which we now compute.

The field F is a degree d extension of the rational numbers $\mathbb{Q}$ and it is the smallest field extension of $\mathbb{Q}$ containing π. Having fixed $\pi \in \mathbb{C}$, we obtain an embedding $F \subset \mathbb{C}$. However it actually admits d different embeddings into the complex numbers, $\sigma_i : F \to \mathbb{C}$ which are determined by setting $\sigma_i(\pi) = \zeta^i \pi$ (for $0 \leq i \leq d-1$) where $\zeta \in \mathbb{C}$ is a primitive d-th root of unity. The norm $\mathsf{N}(u)$ of an element $u \in F$ is the product of the images of u under these embeddings. (These facts use the irreducibility of the polynomial $x^d - N$.) Hence, $\mathsf{N}(\pi) = \pi^d \zeta^{d(d-1)/2} = \pm N$, which proves the claim. (We remark in passing that $1/\pi = \pi^{d-1}/N$ so the field $F = \mathbb{Q}(\pi) = \mathbb{Q}[\pi]$ consists of polynomials in π with rational coefficients.)

Having found a complete set of representatives for $R/(\pi)$ we can now describe the completion R_π. Each $a \in R_\pi$ can be uniquely represented as a power series $a = a_0 + a_1\pi + \cdots$ with coefficients $a_i \in S = \{0, 1, 2, \cdots, N-1\}$, however we must remember that $N = \pi^d$. Consequently, addition of π-adic integers may be described as termwise addition with a "delayed carry": each carried quantity is delayed d steps before adding it back in. In other words, if $b = b_0 + b_1\pi + \cdots$ then

$$a + b = \sum_{i=0}^{\infty} e_i \pi^i,$$

with $0 \leq e_i \leq N-1$, means that there exist $c_d, c_{d+1}, \cdots \in \{0, 1\}$ with

$$a_i + b_i + c_i = e_i + N c_{i+d}.$$

That is, c_i is the carry to the ith position. Similarly the difference $a - b = \sum_{i=0}^{\infty} f_i \pi^i$ is obtained by subtracting the coefficients symbol by symbol, using a "borrow" operation which is delayed d steps. The "borrow" operation is actually the same as the "carry" operation, but the carried quantity is negative. That is,

$$a_i - b_i + c_i = e_i + N c_{i+d}$$

from which it also follows immediately that the amount c_i to be carried to the ith place is either 0 or -1. In this case it is possible to improve on Proposition 4.5.4.

Proposition 4.5.5. *As a subset of F, the intersection $R_\pi \cap F$ consists of all elements u/q such that $u, q \in F$ and q, π are coprime. As a subset of R_π the intersection $R_\pi \cap F$ consists of all elements $a = a_0 + a_1\pi + \cdots$ whose coefficient sequence $\mathbf{seq}_\pi(a) = a_0, a_1, \cdots$ is eventually periodic.*

Proof. The first statement is Proposition 4.5.4. If $a \in R_\pi$ is an element whose coefficient sequence is eventually periodic with period m, then using the geometric series, it follows that $a = h/(1-\pi^m) \in F$ (for some $h \in R$). On the other hand, suppose that $u/q \in F$ (and q is relatively prime to π). The ring $\mathbb{Z}[\pi]/(q)$ is finite by Lemma 2.4.8. Therefore the elements $\{1, N, N^2, \cdots\}$ are not all distinct (mod q) which implies that $N^r \equiv 1 \pmod{q}$ for some $r \geq 1$. Hence there exists $a \in \mathbb{Z}[\pi]$ such that $aq = 1 - N^r$ so $u/q = ua/(1 - N^r)$. Set $ua = v_0 + v_1\pi + \cdots + v_{d-1}\pi^{d-1}$ with $v_i \in \mathbb{Z}$.

Each $v_i/(1-N^r) \in \mathbb{Z}_N$ is an N-adic integer whose coefficient sequence is eventually periodic, of period (a divisor of) r. These series exactly interleave in the sum

$$\frac{u}{q} = \sum_{i=0}^{d-1} v_i(1 + \pi^{dr} + \pi^{2dr} + \cdots)\pi^i \in R_\pi$$

giving a π-adic number whose coefficient sequence is eventually periodic of period rd. □

Even if the coefficient sequences of $a, b \in R_\pi$ are strictly periodic of the same period, say T, the same is not necessarily true for the coefficient sequences of $a \pm b$. Since the carries are delayed for d steps, the periodic part of $a \pm b$ might begin only after d symbols have passed.

Lemma 4.5.6. *Let*

$$a = \sum_{i=0}^{\infty} a_i\pi^i \quad \text{and} \quad b = \sum_{i=0}^{\infty} b_i\pi^i$$

be π-adic integers whose coefficient sequences are eventually periodic with period (a divisor of) n. Then the coefficient sequence of $a \pm b$ is eventually periodic with period (a divisor of) n.

Proof. (We consider the case of $a - b$; the case of the sum is similar.) It suffices to show that the sequence of carries $c_0, c_1, \ldots$ is eventually periodic with period dividing n. Suppose a carry occurs in the ith place, i.e. $c_i = -1$. This occurs if and only if for some positive $k \leq i/d$ we have $a_{i-jd} = b_{i-jd}$ for $1 \leq j \leq k-1$, $a_{i-kd} = 0$, and $b_{i-kd} = 1$. But if this occurs then the same is true with i replaced by $i + rn$ for every positive integer r.

Thus there are two possibilities for any i. Either for all r there is no carry to position $i + rn$, or for r large enough there is a carry to position $i + sn$ for every $s \geq r$. Therefore the sequence of carries has eventual period dividing n, and the lemma follows. □

4.6 Other constructions

In this section we describe other ways to define the π-adic integers over an integral domain R. We include this material for completeness but the results in this section will not be used in the sequel.

4.6.a R_π as an inverse limit

The collection of rings $\{R^i = R/(\pi^i) : 1 \leq i < \infty\}$ forms a directed system with (the reduction moduli π^i) homomorphisms $\psi_{j,i} : R^j \to R^i$ for $i \leq j$. So the limit $\varprojlim \{R^i\}$ exists (see Section 1.2.l), and there are projections $\varphi_i : \varprojlim \{R^i\} \to R^i$ such that $\phi_i = \psi_{j,i} \circ \phi_j$ whenever $i \leq j$. Similarly, the ring R_π comes with (reduction modulo π^i) homomorphisms $\psi_i : R_\pi \to R^i$ such that $\psi_i = \psi_{j,i} \circ \psi_j$.

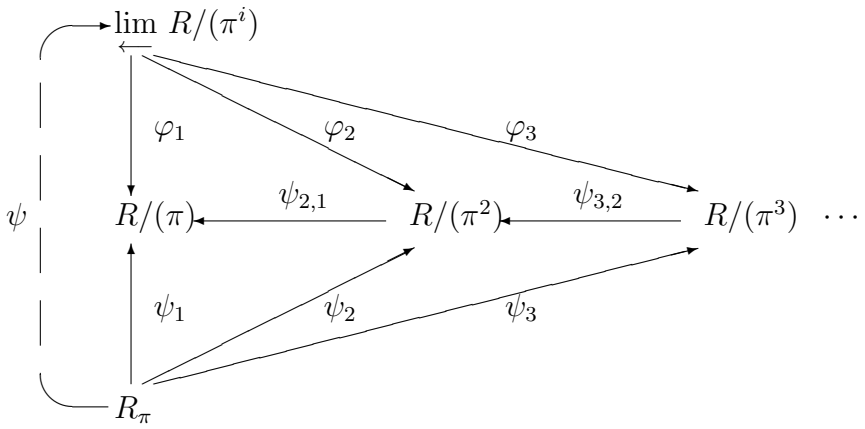


Figure 4.3: R_π as an inverse limit

Consequently there exists a homomorphism $\psi : R_\pi \to \varprojlim \{R_i\}$ such that $\psi_i = \varphi_i \circ \psi$, see Figure 4.3.

Proposition 4.6.1. *The function $\psi : R_\pi \to \varprojlim \{R/(\pi^i)\}$ is an isomorphism of rings.*

Proof. If $a = \sum_{i=0}^{\infty} a_i \pi^i \in R_\pi$ is nonzero, then π^n does not divide $\sum_{i=0}^{n-1} a_i \pi^i$ for some n. Thus $\psi_n(a) \neq 0$, and therefore $\psi(a) \neq 0$. This implies ψ is injective. Let $b = (b_0, b_1, \cdots) \in \varprojlim \{R/(\pi^i)\}$. For each i let $c_i \in R$ reduce to b_i modulo π^i. Thus $\pi^i | (c_i - c_{i-1})$. Let $a_i = (c_i - c_{i-1})/\pi^i$. Then $a = \sum_{i=0}^{\infty} a_i \pi^i$ reduces to b_i modulo π^{i+1} for every i. That is, $\psi(a) = b$ and ψ is a surjection and thus an isomorphism. □

Corollary 4.6.2. *Let M be an Abelian group. For $i = 1, 2, \cdots$ let $\tau_i : M \to R/(\pi^i)$ be group homomorphisms satisfying $\tau_i = \psi_{j,i} \circ \tau_j$ whenever $i \leq j$. Then there is a unique homomorphism $\tau : M \to R_\pi$ so that $\tau_i = \psi_i \circ \tau$ for $i = 1, 2, \cdots$. If M is also a module over R (respectively, a ring) and the τ_i are R-module homomorphisms (resp., ring homomorphisms), then so is τ.*

Corollary 4.6.3. *Let R and S be commutative rings with nonunits $\pi \in R$ and $\rho \in S$. Suppose that $\mu : R \to S$ is a ring homomorphism such that $\mu(\pi)$ is divisible by ρ. Then μ extends to a homomorphism $\mu : R_\pi \to S_\rho$.*

Proof. By hypothesis, for each i there is a series of homomorhisms

$$R_\pi \to R_\pi/(\pi^i) = R/(\pi^i) \to S/(\rho^i)$$

so that all the usual diagrams commute. Thus the universal property of S_ρ implies that μ extends to $\mu : R_\pi \to S_\rho$. □

4.6.b Valuations

In many cases the ring R_π may be described as a *completion* with respect to a *discrete valuation*. This important notion is central in much of modern number theory and algebraic geometry.

Definition 4.6.4. *Let A be a ring.* A valuation on A *(sometimes called a "discrete exponential valuation") is a function $\nu : A \to \mathbb{Z} \cup \{\infty\}$ such that for all $a, b \in A$*

1. $\nu(a+b) \geq \min(\nu(a), \nu(b))$.
2. $\nu(ab) = \nu(a) + \nu(b)$.
3. $\nu(a) = \infty$ *if and only if* $a = 0$.

It follows that $\nu(1) = 0$ so $\nu(a^{-1}) = -\nu(a)$ if $a \in A$ is invertible. The valuation is *nontrivial* if there exists a nonzero $a \in A$ such that $\nu(a) > 0$. Let (A, ν) be a ring with a nontrivial valuation. Then A is an integral domain (for if $ab = 0$ then $\infty = \nu(0) = \nu(ab) = \nu(a) + \nu(b)$ so at least one of $\nu(a), \nu(b)$ is ∞). If K is the field of fractions of A, then the valuation extends to a valuation on K by $\nu(a/b) = \nu(a) - \nu(b)$.

Conversely, if (F, ν) is a field with a (nontrivial discrete exponential) valuation ν then the following statements can be checked.

1. The set $F_{\geq 0} = \{a \in F : \nu(a) \geq 0\}$ is a ring with valuation, called the *valuation ring* of the field. For every $a \in F$, at least one of $a \in F_{\geq 0}$ or $a^{-1} \in F_{\geq 0}$.
2. If $S^{-1}F_{\geq 0}$ denotes the fraction field of $F_{\geq 0}$ then the mapping $h : S^{-1}F_{\geq 0} \to F$ given by $h(a/b) = ab^{-1}$ is an isomorphism of fields (with valuation).
3. There is exactly one maximal ideal in $F_{\geq 0}$ and it is the set $I = F_{>0} = \{a : \nu(a) > 0\}$. Consequently $F_{\geq 0}$ is a *local ring*, and an element $a \in F_{\geq 0}$ is invertible if and only if $\nu(a) = 0$. Moreover, $\cap_{i=0}^{\infty} I^n = \{0\}$, cf. equation (4.12).
4. The quotient $F_{\geq 0}/F_{>0}$ is a field, called the *residue field*,.

Examples:

1. Let K be a field and $F = K((x))$ its field of formal Laurent series. If

$$a(x) = a_m x^m + a_{m+1}x^{m+1} + a_{m+2}x^{m+2} + \cdots \in F$$

is a series with leading term $a_m \neq 0$, set $\nu(a(x)) = m$ (which can be positive, zero, or negative). Then ν is a discrete valuation on F and its valuation ring is the ring of formal power series $F[[x]]$, with maximal ideal (x). The residue field is K.

2. Let p be a prime integer. If $a \in \mathbb{Z}$ is an integer then we have $a = p^n b$ for some nonnegative integer n and some integer b that is relatively prime to p. Define $\nu_p(a) = n$. Then ν_p is a valuation on $\mathbb{Z}$. This valuation extends to the fraction field $\mathbb{Q}$ and its valuation ring is $\mathbb{Q}_{\geq 0} = \mathbb{Z}_{p,0}$, the set of fractions a/b (in lowest terms) such that b is not divisible by p, cf. Section 4.4.c. The maximal ideal in $\mathbb{Z}_{p,0}$ is (p) and the residue field is $\mathbb{F}_p = \mathbb{Z}/(p)$. We remark that this procedure does not give a valuation if p is replaced by a composite integer, say, $N = ab$ with $a, b \in \mathbb{Z}$. For then $\nu_N(a) = \nu_N(b) = 0$ (since N does not divide a or b), but $\nu(N) = 1$.

3. Let $p \in \mathbb{Z}$ be a prime integer and let $\mathbb{Q}_p$ be the field of p-adic numbers. If $a = a_m p^m + a_{m+1} p^{m+1} + \cdots$ with leading term $a_m \neq 0$, set $\nu_p(a) = m$. Then ν_p is a valuation on $\mathbb{Q}_p$; its restriction to $\mathbb{Q} \subset \mathbb{Q}_p$ agrees with the valuation ν_p described in item (2) above. The valuation ring is $\mathbb{Z}_p$, the p-adic integers, and the residue field is $\mathbb{F}_p = \mathbb{Z}/(p)$.

4. More generally, let R be a UFD with fraction field F, and let $\pi \in R$ be prime. If $a \in R$, then $a = \pi^n b$ for some nonnegative integer n and some $b \in R$ not divisible by π. If we define $\nu_\pi(a) = n$, then ν_π is a valuation on R. It extends to a valuation on F by $\nu(c/d) = \nu(c) - \nu(d)$. Similarly, it extends to valuations on R_π and F_π. Moreover, $R_\pi = (F_\pi)_{\geq 0}$.

5. Let (F, ν) be a discretely valued field with valuation ring $R_\nu = F_{\geq 0}$ and maximal ideal $I_\nu = F_{>0}$. Let $\pi \in I_\nu$ be an element whose valuation is minimal, say $\nu(\pi) = c$. Then π is prime in R_ν, and every element $y \in F$ is of the form $y = \pi^a x$ with $\nu(x) = 0$, and $\nu(y) = ac$. In other words, the construction in example (4) is completely general. To see this, first suppose that $\nu(y) = ac + d$ with $0 < d < c$. Then $\nu(y/\pi^a) = d$ which contradicts the minimality of c, hence $d = 0$. Therefore $b = y/\pi^a$ is a unit, and $y = b\pi^a$ as claimed. Similarly, if $\pi = uv$ is a nontrivial product (with $u, v \in R_\nu$, neither of which is a unit) then $\nu(\pi) = \nu(u) + \nu(v) \geq 2c$ which is false, so π is prime in R_ν.

4.6.c Completions

A *metric space* is a set X with a *metric* or "distance function" $\delta : X \times X \to \mathbb{R}$ such that $\delta(a, b) = \delta(b, a)$; $\delta(a, b) = 0$ if and only if $a = b$; and $\delta(a, b) \leq \delta(a, c) + \delta(c, b)$ (triangle inequality) for all $a, b, c \in X$. The *metric topology* on X is the topology generated by the open "balls" $B_\epsilon(x) = \{y \in X : \delta(x, y) < \epsilon\}$ for all $x \in X$ and all $\epsilon > 0$. The metric δ is continuous with respect to this topology. A mapping $f : (X, \delta_X) \to (Y, \delta_Y)$ between metric spaces is *isometric* if $\delta_Y(f(x_1), f(x_2)) = \delta_X(x_1, x_2)$ for all $x_1, x_2 \in X$. Such a mapping is continuous with respect to the metric topologies on X and Y. An *isometry* $f : (X, \delta_X) \to (Y, \delta_Y)$ is an isometric mapping that has an isometric inverse. (In particular, it is one to one and onto.)

A sequence of points $x_1, x_2, \cdots$ in a metric space X is a *Cauchy sequence* if for every $\epsilon > 0$ there exists a k so that $\delta(x_i, x_j) < \epsilon$ if $i, j \geq k$. A metric space is *complete* if every Cauchy

sequence converges. A *completion* $(\widehat{X}, \widehat{\delta})$ of a metric space (X, δ) is a complete metric space that contains X as a dense subset, such that the restriction of $\widehat{\delta}$ to X equals δ. Every metric space has a completion (constructed below). If $(\widehat{X}_1, \widehat{\delta}_1)$ and $(\widehat{X}_2, \widehat{\delta}_2)$ are two completions of a metric space (X, δ) then the identity mapping $X \to X$ extends in a unique way, to a continuous mapping $\widehat{f} : (\widehat{X}_1, \widehat{\delta}_1) \to (\widehat{X}_2, \widehat{\delta}_2)$ and moreover, the mapping $\widehat{f}$ is an isometry.

Thus, the completion of (X, δ) is unique up to isometry. It may be constructed as follows. The points in $\widehat{X}$ are equivalence classes of Cauchy sequences in X, two sequences $\mathbf{x} = x_1, x_2, \cdots$ and $\mathbf{y} = y_1, y_2, \cdots$ being equivalent if

$$\lim_{i \to \infty} \delta(x_i, y_i) = 0.$$

If $\mathbf{z} = z_1, z_2, \cdots$ is another point in $\widehat{X}$ then the extended metric is defined by $\widehat{\delta}(\mathbf{x}, \mathbf{z}) = \lim \delta(x_i, z_i)$ (which exists because $\mathbf{x}, \mathbf{z}$ are Cauchy sequences). The space X is contained in $\widehat{X}$ as the set of constant sequences.

Two metrics δ_1, δ_2 on a set X are *equivalent* if the set of Cauchy sequences for δ_1 coincides with the set of Cauchy sequences for δ_2. In this case, the identity mapping $I : X \to X$ has a unique continuous extension to the completions, $\widehat{I} : (\widehat{X}, \widehat{\delta}_1) \to (\widehat{X}, \widehat{\delta}_2)$ and $\widehat{I}$ is a homeomorphism.

Lemma 4.6.5. *Let ν be a discrete valuation on a field F and let $q > 1$ be a positive real number. Then $\delta(a, b) = q^{-\nu(a-b)}$ defines a metric on F. A different choice of $q > 1$ determines an equivalent metric. Moreover, for any Cauchy sequence $x_1, x_2, \cdots$ the limit $\lim \nu(x_i) \in \mathbb{Z} \cup \infty$ exists, and if the limit is not ∞ then it is attained after finitely many terms.*

Proof. If $\delta(a, b) = 0$ then $\nu(a - b) = \infty$ so $a = b$. If $a, b, c \in F$ then

$$\delta(a, b) = q^{-\nu(a-c+c-b)} \leq \max(q^{-\nu(a-c)}, q^{-\nu(c-b)}) \leq q^{-\nu(a-c)} + q^{-\nu(c-b)} = \delta(a, c) + \delta(c, b)$$

so δ is a metric. Now let $x_1, x_2, \cdots$ be a Cauchy sequence. This means that for any $T \geq 1$ there is a $k \geq 1$ such that

$$\nu(x_i - x_j) \geq T \quad \text{whenever} \quad i, j \geq k. \tag{4.14}$$

(So the particular choice of q does not matter.) There are now two possibilities. The first is that for infinitely many values of i, the values of $\nu(x_i)$ grow without bound. This in fact implies that $\nu(x_i) \to \infty$ (so $x_i \to 0$) because, for all i, j,

$$\nu(x_j) = \nu(x_i + (x_j - x_i)) \geq \min\{\nu(x_i), \nu(x_j - x_i)\}. \tag{4.15}$$

Since $\nu(x_i)$ can be chosen to be arbitrarily large, and since $\nu(x_i - x_j)$ grows without bound, it follows that $\nu(x_j)$ grows without bound.

The second possibility, therefore, is that the values of $\nu(x_i)$ remain bounded for all i. Consequently there exists $0 \leq M < \infty$ so that $\nu(x_j) \leq M$ for all j sufficiently large, and so that

$\nu(x_i) = M$ for infinitely many values of i. So there is an index i_0 with the property that $\nu(x_{i_0}) = M$ and if $i, j \geq i_0$ then $\nu(x_i - x_j) > M$. Hence, by equation (4.15), $\nu(x_j) = M$ whenever $j \geq i_0$, that is, the sequence $\nu(x_j)$ converges to M and it equals M after finitely many terms have passed. □

If the discretely valued field (F, ν) is complete with respect to the metric defined by ν, then we say that (F, ν) is a *complete discretely valued field* or *local field*.

Theorem 4.6.6. *Let (F, ν) be a field with a discrete valuation, with associated metric δ as in Lemma 4.6.5, and with valuation ring $R = F_{\geq 0}$. Then the valuation ν extends to a valuation $\widehat{\nu}$ on the completion $\widehat{F}$. Moreover, $\widehat{F}$ is again a field (so it is a local field) and its valuation ring $\widehat{F}_{\geq 0}$ naturally identifies with the completion $\widehat{R}$. In particular, $\widehat{F}$ is the fraction field of $\widehat{R}$. We say that $\widehat{F}$ is the* completion *of F with respect to ν.*

Proof. Let $\mathbf{x} = x_1, x_2, \cdots$ be a Cauchy sequence. By Lemma 4.6.5 the sequence $\nu(x_1), \nu(x_2), \cdots$ converges so we may define $\widehat{\nu}(\mathbf{x}) = \lim_{i\to\infty} \nu(x_i)$. If $\mathbf{y} = y_1, y_2, \cdots$ is an equivalent Cauchy sequence then $\widehat{\nu}(\mathbf{y}) = \widehat{\nu}(\mathbf{x})$ so $\widehat{\nu}$ is a well defined valuation on the completion $\widehat{F}$.

Let T be the set of all Cauchy sequences in F. Then T is a subring of the product of infinitely many copies of F, that is, addition and multiplication of two sequences is defined termwise. We need to check that these arithmetic operations are preserved by the equivalence relation on Cauchy sequences. The set of Cauchy sequences with limit 0 is an ideal I in T. Observe that two Cauchy sequences $\mathbf{x} = x_1, x_2, \cdots$ and $\mathbf{y} = y_1, y_2, \cdots$ are equivalent if and only if

$$0 = \lim_{i\to\infty} \delta(x_i, y_i) = q^{-\nu(x_i - y_i)}$$

which holds if and only if $\nu(x_i - y_i) \to \infty$, that is, $x_i - y_i \in I$. Thus, the completion $\widehat{F}$ is exactly T/I, which is a ring. To see that it is a field we need to show that every nonzero element has an inverse. Let $\mathbf{x} = x_1, x_2, \cdots$ be a Cauchy sequence that does not converge to 0. By Lemma 4.6.5 the sequence $\nu(x_i)$ converges to some number M and it equals M after some finite point. Therefore if i, j are sufficiently large,

$$\nu\left(\frac{1}{x_i} - \frac{1}{x_j}\right) = \nu\left(\frac{x_j - x_i}{x_i x_j}\right) = \nu(x_i - x_j) - \nu(x_i) - \nu(x_j) = \nu(x_i - x_j) - 2M \to \infty.$$

This shows that the sequence $x_1^{-1}, x_2^{-1} \cdots$ is a Cauchy sequence, and it therefore represents $\mathbf{x}^{-1} \in \widehat{F}$.

In a similar way we obtain the completion $\widehat{R} \subset \widehat{F}$ of the valuation ring $R = F_{\geq 0}$ and Lemma 4.6.5 implies that $\widehat{R} \subset \widehat{F}_{\geq 0}$. Conversely, if $\mathbf{x} \in \widehat{F}$ and if $\widehat{\nu}(\mathbf{x}) \geq 0$ then, again by Lemma 4.6.5, this implies that $\nu(x_i) \geq 0$ for all sufficiently large i, say, $i \geq i_0$. Therefore, if we replace $\mathbf{x}$ by the equivalent Cauchy sequence $\mathbf{x}' = x_{i_0}, x_{i_0+1}, \cdots$ then $\mathbf{x}' \in \widehat{R}$, which proves that $\widehat{F}_{\geq 0} = \widehat{R}$. □

Remarks. Completeness is not a "purely topological" invariant: it depends on a choice of metric as well. The real numbers $\mathbb{R}$ is complete (with the usual metric) but the open interval $(0,1)$, which is homeomorphic to $\mathbb{R}$, is not complete. Its completion is the closed interval. The set of real numbers is the completion of the rational numbers with respect to the Euclidean metric $\delta(x,y) = |x-y|$, however this metric does not arise from a *discrete* valuation. The following theorem says that the π-adic numbers as constructed in Section 4.5 is an example of a completion.

Theorem 4.6.7. *Let R be a UFD with field of fractions F. Let $\pi \in R$ be prime and let ν_π be the corresponding discrete valuation as in example 4 of Section 4.6.b. Then (R_π, ν_π) is isomorphic to its completion $(\widehat{R}, \widehat{\nu}_\pi)$, and F_π is isomorphic to its completion $(\widehat{F}, \widehat{\nu}_\pi)$.*

Proof. Let $\mathbf{x} = x_1, x_2, \cdots \in \widehat{R}$ be a Cauchy sequence. For each fixed n the sequence of reductions $x_i \pmod{\pi^n} \in R/(\pi^n)$ eventually stabilizes, giving a collection of compatible homomorphism $\widehat{R} \to R/(\pi^n)$. By Corollary 4.6.2 this gives a homomorphism $\widehat{R} \to R_\pi$. The inverse homomorphism associates to each power series $\sum_{i=0}^{\infty} a_i \pi^i$ its sequence of partial sums $a_0, a_0 + a_1\pi, \cdots$ which is a Cauchy sequence. Thus ψ is an isomorphism of complete valued rings, so its canonical extension $\psi : \widehat{F} \to F_\pi$ is an isomorphism of the corresponding fraction fields. □

A basic property of local fields is expressed in *Hensel's Lemma* which allows us to factor a polynomial over the residue field, and to lift the factorization to the local field. Let F be a complete discretely valued field with discrete valuation ν, valuation ring $R = F_{\geq 0}$, maximal ideal $I = F_{>0}$ and residue field $K = F_{\geq 0}/F_{>0}$ (all depending on ν) as in Section 4.6.b. If $f(x)$ is a polynomial over R, we denote by $\bar{f}(x)$ the reduction of $f(x)$ modulo the ideal I. The proof of the following may be found, for example, in [15, pp. 573-4].

Theorem 4.6.8. *(Hensel's Lemma) Suppose $f(x) \in R[x]$ is a monic polynomial and $\bar{f}(x) = g_0(x)h_0(x)$ in $K[x]$, where $g_0(x)$ and $h_0(x)$ are monic and relatively prime. Then there exist monic polynomials $g(x)$ and $h(x)$ in $R[x]$ such that $f(x) = g(x)h(x)$, $\bar{g}(x) = g_0(x)$, and $\bar{h}(x) = h_0(x)$.*

Corollary 4.6.9. *With the same hypotheses, if $\bar{f}(x)$ has a simple root a_0, then $f(x)$ has a simple root a such that $a \pmod{I} = a_0$.*

4.6.d Adic topology

The construction of R_π using valuations only works when R is a UFD and π is prime. But a similar construction works for more general ideals in more general rings. Let R be an integral domain and let $I \subset R$ be an ideal. Suppose that R is *separable* with respect to I, that is, $\cap_{n=1}^{\infty} I^n = \{0\}$. If $x \in I$ define $V(x) = \sup\{n : \ x \in I^n\} \in \mathbb{Z} \cup \infty$. If $x, y \in I$ then $V(x+y) \geq \min\{V(x), V(y)\}$ and $V(xy) \geq V(x) + V(y)$ (compare with Section 4.6.4). Fix $q > 1$ and define

$$\delta(x,y) = \begin{cases} q^{-V(x-y)} & \text{if } \ x - y \in I \\ \infty & \text{otherwise.} \end{cases}$$

Then V is almost a valuation, although it is not defined on all of R. However, the same method as in Lemma 4.6.5 and Theorem 4.6.6 shows that δ is a metric on R. It determines a topology on R, a basis of which is given by the open sets of the form $B_n(x) = x + I^n$ for $x \in R$ and $n \geq 1$. If $I = (\pi)$ is principal we refer to δ as a π-adic metric, and to the resulting topology as the π-adic topology.

Theorem 4.6.10. *Let R be an integral domain and let $\pi \in R$. Suppose R is separable with respect to the ideal (π). Then the ring R_π of π-adic integers may be naturally identified with the completion of R in the π-adic metric.*

Proof. The proof is the same as that of Theorem 4.6.7. □

4.7 Continued fractions

Continued fraction expansion provides an alternate way to represent certain algebraic objects. Every real number x has a continued fraction expansion. The continued fraction expansion of a rational number a/b is equivalent to Euclid's algorithm (300 BC) for (a, b). Specific examples of continued fractions were known to Bombelli and Cataldi around 1600. The first systematic treatment of continued fractions was by John Wallis in Opera Mathematica (1695). The subject was intensively studied in the nineteenth century. Like the Euclidean algorithm, the continued fraction expansion is optimal in two ways: (a) the successive terms, or "convergents" in this expansion give best-possible rational approximations to x, see Theorem 4.7.4; and (b) the terms in the expansion can be computed with very little effort. There are many wonderful applications of continued fractions to problems in mathematics, science, and engineering. For example, in [2] a constant is estimated, using a hand calculator, to be 2.1176470588. The CF expansion for this number is $[2, 8, 2, 147058823]$, suggesting that the actual number is $[2, 8, 2] = 36/17$, which turns out to be correct. In [8], continued fractions are used to describe the efficacy of the twelve-tone equal tempered musical scale, with the next best equal tempered scale having 19 tones.

Standard references for continued fractions include [11], [16] and [27]. We shall not explore this topic in detail, but we develop enough of the theory to understand the relation between continued fractions and the Berlekamp-Massey algorithm for linear feedback shift register synthesis.

4.7.a Continued fractions for rational numbers

The continued fraction representation for a rational number a/b (with a, b positive integers) is defined by the iterative procedure in Figure 4.4. Let $a_0 = a, a_1, a_2, \cdots$ and $b_0 = b, b_1, b_2, \cdots$ be the

RatContFrac(a, b)
begin
$n = 0$
while $b \neq 0$ **do**
Let $\frac{a}{b} = c_n + \frac{a'}{b}$ with $c_n, a' \in \mathbb{Z}$ and $0 \leq a' < b$
$a = b$
$b = a'$
$n = n + 1$
od
return $\langle c_0, c_1, \cdots, c_{n-1} \rangle$
end

Figure 4.4: Rational Continued Fraction Expansion.

sequences of as and bs generated by the algorithm, then we have successively

$$\frac{a}{b} = c_0 + \frac{a'}{b} = c_0 + \frac{b_1}{a_1} = c_0 + \frac{1}{\frac{a_1}{b_1}} = c_0 + \frac{1}{c_1 + \frac{b_2}{a_2}} = c_0 + \frac{1}{c_1 + \frac{1}{c_2 + \frac{a_3}{b_3}}} = \cdots$$

which we denote $[c_0, c_1, c_2 \cdots]$. If $a/b = 10/7$, this gives $\frac{10}{7} = 1 + \frac{3}{7} = 1 + \frac{1}{2 + \frac{1}{3}}$, so the continued fraction expansion of $10/7$ is $[1, 2, 3]$.

Proposition 4.7.1. *The procedure in algorithm* RatContFrac *halts after finitely many steps.*

Proof. We always have $b > a'$, so after the first iteration $a' < a$. Therefore, for every i we have $\max(a_{i+2}, b_{i+2}) < \max(a_i, b_i)$. It follows that eventually $b = 0$ and the algorithm halts. □

The sequence of non-negative integers $[c_0, c_1, \cdots, c_{n-1}]$ is called the *continued fraction expansion of* a/b. It is uniquely defined and gives an exact representation of a/b. Similarly, we can generate continued fraction expansions of real numbers. If $z > 0$ is real, let $\{z\}$ denote the fractional part of z and let $[z]$ denote the integer part or floor of z. Thus $z = [z] + \{z\}$. Then the continued fraction expansion of z is the sequence generated by the recursive definition

$$c_0 = [z], \quad r_0 = \{z\} = z - c_0$$

and for $n \geq 1$,

$$z_n = \frac{1}{r_{n-1}}, \quad c_n = [z_n], \quad r_n = \{z_n\}, \quad \text{so } z_n = c_n + r_n \tag{4.16}$$

where we continue only as long as $r_n \neq 0$. If z is irrational, then this recursion does not halt, but outputs an infinite sequence of integers $[c_0, c_1, \cdots]$ which is called the *continued fraction expansion of* z. For example, the continued fraction expansion of $z_0 = \sqrt{7}$ is:

$$\begin{aligned} z_0 &= 2 + (\sqrt{7} - 2) & z_1 &= \frac{1}{\sqrt{7}-2} = 1 + \frac{\sqrt{7}-1}{3} \\ z_2 &= \frac{3}{\sqrt{7}-1} = 1 + \frac{\sqrt{7}-1}{2} & z_3 &= \frac{2}{\sqrt{7}-1} = 1 + \frac{\sqrt{7}-2}{3} \\ z_4 &= \frac{3}{\sqrt{7}-2} = 4 + (\sqrt{7} - 2) & z_5 &= z_1. \end{aligned}$$

Thus the expansion repeats from here on, and the continued fraction is $[2, 1, 1, 1, 4, 1, 1, 1, 4, \cdots]$.

The *nth convergent* of the continued fraction $[c_0, c_1, \cdots]$ is the rational number f_n/q_n that is obtained from the finite continued fraction $[c_0, c_1, \cdots, c_n]$. The convergents f_n/q_n form a sequence of rational approximations to z. The following proposition, when combined with the algorithm of equation (4.16) or Figure 4.4 provides an efficient way to compute the convergents.

Proposition 4.7.2. *Let $z > 0$ be a real number with continued fraction expansion $z = [c_0, c_1, \cdots]$. Let r_n be the remainder as in equation (4.16). Then the convergents may be obtained from the following recursive rule: if $r_n \neq 0$ then*

$$f_{n+1} = c_{n+1} f_n + f_{n-1} \quad \text{and} \quad q_{n+1} = c_{n+1} q_n + q_{n-1}. \tag{4.17}$$

The initial conditions are: $f_0 = c_0$, $q_0 = 1$, $f_{-1} = 1$, and $q_{-1} = 0$. Moreover, for any n,

$$z = \frac{f_n + f_{n-1} r_n}{q_n + q_{n-1} r_n}. \tag{4.18}$$

Proof. At the nth stage of the recursion we have a representation

$$z = c_0 + (c_1 + (c_2 + \cdots + (c_{n-1} + (c_n + r_n)^{-1})^{-1} \cdots)^{-1})^{-1}.$$

The dependence on the innermost quantity, $(c_n + r_n)$, is fractional linear:

$$z = \frac{u_n(c_n + r_n) + w_n}{x_n(c_n + r_n) + y_n}, \tag{4.19}$$

where u_n, w_n, x_n, y_n are multilinear expressions in $c_0, \cdots, c_{n-1}$. Then f_n/q_n is obtained by setting $r_n = 0$ in equation (4.19), so

$$\frac{f_n}{q_n} = \frac{u_n c_n + w_n}{x_n c_n + y_n}.$$

That is, $f_n = u_n c_n + w_n$ and $q_n = x_n c_n + y_n$. Now consider equation (4.19) with n replaced by $n+1$. This gives the same result as equation (4.19) with $r_n \neq 0$ replaced by $(c_{n+1} + r_{n+1})^{-1}$. Thus

$$\begin{aligned}
\frac{u_{n+1}(c_{n+1} + r_{n+1}) + w_{n+1}}{x_{n+1}(c_{n+1} + r_{n+1}) + y_{n+1}} &= \frac{u_n(c_n + (c_{n+1} + r_{n+1})^{-1}) + w_n}{x_n(c_n + (ca_{n+1} + r_{n+1})^{-1}) + y_n} \\
&= \frac{u_n(c_n(c_{n+1} + r_{n+1}) + 1) + w_n(c_{n+1} + r_{n+1})}{x_n(c_n(c_{n+1} + r_{n+1}) + 1) + y_n(c_{n+1} + r_{n+1})} \\
&= \frac{(u_n c_n + w_n)(c_{n+1} + r_{n+1}) + u_n}{(x_n c_n + y_n)(c_{n+1} + r_{n+1}) + x_n}.
\end{aligned}$$

This being an equality of rational functions, we may conclude that $u_{n+1} = u_n c_n + w_n$ and that $w_{n+1} = u_n$. But $u_n c_n + w_n = f_n$ hence $u_{n+1} = f_n$ (and therefore $u_n = f_{n-1}$). Similarly $x_{n+1} = x_n c_n + y_n = q_n$, and $y_{n+1} = x_n = q_{n-1}$. Equation (4.17) follows immediately and equation (4.19) becomes (4.18). □

Lemma 4.7.3. *If $n \geq 0$ and $r_n \neq 0$ then $f_{n+1}q_n - q_{n+1}f_n = (-1)^{n+1}$ so f_n and q_n are relatively prime.*

Proof. The proof is by induction on n. The initial conditions give $f_0 q_{-1} - q_0 f_{-1} = 1$. If $n > 1$, then using equations (4.17) we have

$$f_n q_{n+1} - q_n f_{n+1} = f_n(c_{n+1}q_n + q_{n-1}) - q_n(c_{n+1}f_n + f_{n-1}) = -(f_{n-1}q_n - q_{n-1}f_n) = -(-1)^n. \quad \square$$

Theorem 4.7.4. *Let f_n/q_n denote the nth convergent ($n \geq 1$) of $z \in \mathbb{R}$ ($z > 0$). Then*

$$\left| z - \frac{f_n}{q_n} \right| < \frac{1}{q_n q_{n+1}}. \tag{4.20}$$

If $r_n \neq 0$, then $q_{n+1} > q_n$. If f, q are positive integers and if $|z - f/q| < 1/q_n q_{n+1}$, then $q > q_n$ unless $f/q = f_n/q_n$.

Proof. If $r_n = 0$, then $z = f_n/q_n$, so we may assume $r_n \neq 0$. By equation (4.18) we have

$$\begin{aligned}
z - \frac{f_n}{q_n} &= \frac{f_n + f_{n-1}r_n}{q_n + q_{n-1}r_n} - \frac{f_n}{q_n} \\
&= \frac{(f_{n-1}q_n - q_{n-1}f_n)r_n}{q_n(q_n + q_{n-1}r_n)} \\
&= \frac{(-1)^n r_n}{q_n(q_n + q_{n-1}r_n)} \\
&= \frac{(-1)^n}{q_n((1/r_n)q_n + q_{n-1})}.
\end{aligned}$$

For $i \geq 1$ we have $c_i \geq 0$. Thus by equation (4.17), $q_i \geq 0$ for all i. Therefore

$$\frac{1}{r_n} q_n + q_{n-1} \geq c_{n+1} q_n + q_{n-1} = q_{n+1}$$

which proves equation (4.20). If $0 \neq r_n < 1$ then $z_{n+1} > 1$ so $c_{n+1} \geq 1$. Since $q_{n-1} > 0$, equation (4.17) gives $q_n > q_{n-1}$. Although it is not difficult, the proof of the last statement is tedious, and may be found in [11], [16], or [27]. □

4.7.b Continued fractions for (reciprocal) Laurent Series

A theory of continued fractions can be developed whenever we have a subset R (the analog of the "integers") of a field F and a subset $U \subset F$ (of "fractions") so that every element of F can be uniquely written in the form $a + y$ with $a \in R$ and $y \in U$. Let $z \mapsto \{z\}$ be a function from F to U so that for every z we have $z - \{z\} \in R$. The sequences of elements $c_0, c_1, \cdots \in R$ and $r_0, r_1, \cdots \in U$ are defined exactly as in equation (4.16). This point of view is developed in [32], following work of [26] and [22]. In many cases (but not always: see the example in Section 4.7.c) the resulting "rational" approximations converge and they are often the "best" possible. In this section we describe the approach of [32].

Let K be a field. We wish to develop continued fraction expansions for *rational functions* $f(x)/g(x)$ where $f, g \in R = K[x]$ are polynomials. Unfortunately there is no apparent analog to the "integer part" of such a function, which we would like to be a polynomial in x. However a formal Laurent series $h(x) \in K((x))$ is the sum of two pieces: the (finitely many) terms with negative powers of x, plus the infinite series of terms with positive powers of x. We are thus led to consider continued fractions for the field

$$F = K((x^{-1})) = \left\{ \sum_{i=k}^{\infty} a_i x^{-i} : k \in \mathbb{Z}, a_i \in K \right\},$$

of "reciprocal Laurent series", or formal Laurent series in x^{-1}, because the "integer part" will now be a polynomial in x (with positive powers). As in Section 4.3, the field F contains all quotients of polynomials $f(x)/g(x)$. Thus we define

$$\left[\sum_{i=k}^{\infty} a_i x^{-i} \right] = \sum_{i \leq 0} a_i x^{-i} \in R = K[x]$$

and

$$\left\{ \sum_{i=k}^{\infty} a_i x^{-i} \right\} = \sum_{i \geq 1}^{\infty} a_i x^{-i} \in x^{-1} K[[x^{-1}]].$$

That is, the polynomial part of this Laurent series is the sum of the monomials with nonnegative exponents. The fractional part is the sum of the monomials with negative exponents. It is an element in the unique maximal ideal (x^{-1}) in $K[[x^{-1}]]$. With these definitions we can carry out continued fraction expansions just as for the real numbers in equation (4.16). That is,

$$z_n = \frac{1}{r_{n-1}}, \quad c_n = [z_n], \quad r_n = \{z_n\}, \quad \text{so } z_n = c_n + r_n$$

with $c_0 = [z]$ and $r_0 = \{z\}$. (See exercises 16 and 17.) The associated *convergent* f_n/q_n is obtained by stopping at stage n and replacing r_n with 0.

Proposition 4.7.5. *Let $z \in K((x^{-1}))$, let $n \geq 1$ and let f_n/q_n be its nth convergent. Then*

$$f_{n+1} = c_{n+1}f_n + f_{n-1} \quad \textit{and} \quad q_{n+1} = c_{n+1}q_n + q_{n-1}. \tag{4.21}$$

The initial conditions are $f_0 = c_0 = [z]$; $q_0 = 1$; and $f_{-1} = 1$; $q_{-1} = 0$. Moreover,

$$f_{n-1}q_n - q_{n-1}f_n = (-1)^n \tag{4.22}$$

so f_n and q_n are relatively prime. If $z = u/v$ with $u, v \in K[x]$ then the continued fraction expansion of z is finite and its length is at most the degree of v.

Proof. The proof of the first two statements is exactly the same as that of Proposition 4.7.2 and Lemma 4.7.3. For $n \geq 1$, the element r_n can be expressed as a quotient of polynomials with the degree of the numerator less than the degree of the denominator. The numerator at the nth stage is the denominator at the $(n+1)$st stage. Thus the degrees of the denominators are strictly decreasing. This implies the length of the expansion is no more than $\deg(v)$. □

Recall from Section 4.6.b that the field $K((x^{-1}))$ of formal Laurent series admits a metric,

$$\delta(z, w) = 2^{-\nu(z-w)}$$

for $z, w \in K((x^{-1}))$, where ν is the discrete valuation

$$\nu\left(\sum_{i=k}^{\infty} a_i x^{-i}\right) = \min\{i : \ a_i \neq 0\}.$$

If $u \in K[x]$ is a polynomial then $\nu(u) = -\deg(u)$.

Now fix $z \in K((x^{-1}))$. Let f_n/q_n be its nth convergent and set $e_n = \deg(q_n)$. The following theorem says that the continued fraction expansion converges, and that the convergents provide the best rational approximation to z.

Theorem 4.7.6. *For any $n \geq 1$, the power series expansion of z equals that of f_n/q_n in all terms involving x^k for $k > -(e_n + e_{n+1})$. That is, $f_n/q_n \equiv z \pmod{x^{-e_n - e_{n+1}}}$ or equivalently,*

$$\delta\left(z, \frac{f_n}{q_n}\right) \leq 2^{-e_n - e_{n+1}}. \tag{4.23}$$

If $r_n \neq 0$ then $e_{n+1} > e_n$. If $f, q \in K[x]$ are relatively prime and if $\delta(z, f/q) < 2^{-2e_n}$ then $\deg(q) > \deg(q_n)$ unless $f/q = f_n/q_n$.

Proof. If $r_n = 0$ then $z = f_n/q_n$ so to prove (4.23), we may assume that $r_n \neq 0$. As in the proof of Theorem 4.7.4,

$$z - \frac{f_n}{q_n} = \frac{(-1)^n}{q_n((1/r_n)q_n + q_{n-1})} = \frac{(-1)^n}{q_n(q_{n+1} + r_{n+1}q_n)}.$$

We will use the fact that $\nu(x+y) \geq \min(\nu(x), \nu(y))$ and that equality holds if $\nu(x) \neq \nu(y)$. By construction, if $n \geq 0$ we have $\nu(r_n) \geq 1$ so $\nu(1/r_n) \leq -1$ so for $n \geq 1$ we have:

$$\nu(c_n) = \nu((1/r_{n-1}) - r_n) = \nu(1/r_{n-1}) \leq -1.$$

Assuming $r_n \neq 0$ gives $c_{n+1} \neq 0$. By equation (4.21) and induction,

$$-e_{n+1} = \nu(q_{n+1}) = \nu(c_{n+1}q_n + q_{n-1}) < \nu(q_n) = -e_n. \tag{4.24}$$

It follows that $\nu(q_{n+1} + r_{n+1}q_n) = \nu(q_{n+1}) = -e_{n+1}$. Thus $\nu(z - f_n/q_n) = e_n + e_{n+1}$ as claimed.

Now suppose that $f, q \in K[x]$ are relatively prime and that $\nu(z - f/q) > 2e_n$. Assume that $e = \deg(q) \leq e_n = \deg(q_n)$. We must show that $f/q = f_n/q_n$. Assume for the moment that $\deg(f) \leq \deg(q)$ and $\deg(f_n) \leq \deg(q_n)$. (We will remove these assumptions below.) Let

$$\hat{f} = x^{-e}f, \quad \hat{q} = x^{-e}q, \quad \hat{f}_n = x^{-e_n}f_n, \text{ and } \hat{q_n} = x^{-e_n}q_n.$$

Then $\hat{f}, \hat{q}, \hat{f}_n, \hat{q}_n \in K[x^{-1}]$ are polynomials with

$$\frac{f}{q} = \frac{\hat{f}}{\hat{q}}, \text{ and } \frac{f_n}{q_n} = \frac{\hat{f}_n}{\hat{q}_n}.$$

Thus

$$\frac{\hat{f}}{\hat{q}} \equiv \frac{\hat{f}_n}{\hat{q}_n} \pmod{x^{-2e_n - 1}}$$

in the ring $K[[x^{-1}]]$. It follows that

$$\hat{f}\hat{q}_n \equiv \hat{f}_n\hat{q} \pmod{x^{-2e_n-1}}.$$

However, by assumption, the left and right sides of this congruence have degrees $\leq 2e_n$ in x^{-1}, so they are in fact equal. It follows then that $fq_n = f_n q$. Now we can take this as an equation in $K[x]$. Since f and q are relatively prime, f divides f_n and q divides q_n. Since f_n and q_n are relatively prime, f_n divides f and q_n divides q. It follows that $f/q = f_n/q_n$.

Now suppose that $\deg(f) \geq \deg(q)$ (or that $\deg(f_n) \geq \deg(q_n)$). Since $\delta(z, f/q) \leq 1$ this implies that $[z] = [f/q] = [f_n/q_n] = c_0$. So we may subtract off this integral part, and apply the previous case to the fractional part. In other words, let $z' = z - c_0$, $f' = f - c_0 q$, and $f'_n = f_n - c_0 q_n$. Then $\deg(f') < \deg(q)$ and $\deg(f'_n) < \deg(q_n)$, while $\delta(z', f'/q) = \delta(z, f/q)$ and $\delta(z', f'_n/q_n) = \delta(z, f_n/q_n)$. We conclude that $\deg(q) > \deg(q_n)$ unless $f'/q = f'_n/q_n$, in which case, by adding back the integral part c_0, we have $f/q = f_n/q_n$. □

4.7.c Continued fractions for Laurent series and p-adic numbers

Continued fractions can be developed almost identically for the field F of Laurent series in x, $F = K((x)) = \{\sum_{i=k}^{\infty} a_i x^i : a_i \in K\}$. In this case the "integer part" is a polynomial in x^{-1}. Every statement in Section 4.7.b now holds with x^{-1} replaced by x. The terms $c_n = [z_n]$ will be polynomials in x^{-1} and the convergents f_n/q_n will be quotients of polynomials in x^{-1}. By multiplying numerator and denominator by an appropriate power of x, we can convert these into approximations by ordinary rational functions, and the series of approximations will generally differ from that in Section 4.7.b because the metrics on $K((x))$ and $K((x^{-1}))$ are different.

A similar situation exists with the p-adic numbers. We can define continued fraction expansions for $z = \sum_{i=k}^{\infty} a_i 2^i$ with $a_i \in \{0, 1, \cdots, p-1\}$ (and k possibly negative) by taking the "integer part", $[z]$, to be the part involving non-positive powers,

$$[z] = \sum_{i=k}^{0} a_i 2^i \quad \text{and} \quad \{z\} = \sum_{i=1}^{\infty} a_i 2^i$$

to be the fractional part. The appropriate metric comes from the usual p-adic valuation. However, the set of "integral parts", (polynomials in 2^{-1}) is not closed under addition or multiplication. This leads to continued fraction expansions that do not converge. For example, consider the 2-adic CF expansion for $-1/2 = 2^{-1} + 2^0 + 2^1 + \cdots$. Since $[-1/2] = 2^{-1} + 2^0$ and $\{-1/2\} = 2^1 + 2^2 + \cdots = -2$ we obtain the infinite expansion

$$-\frac{1}{2} = 2^0 + 2^{-1} + \cfrac{1}{2^0 + 2^{-1} + \cfrac{1}{2^0 + 2^{-1} + \frac{1}{\cdots}}}$$

We can find the best rational approximation to a p-adic number using the theory of *approximation lattices*.

4.8 Exercises

1. Let $F = \mathbb{Q}$ be the rational numbers and $q(x) = x - \frac{1}{2}$. Show that the power series expansion of $1/q(x)$ is not eventually periodic.

2. Let F be a field and suppose that k is a positive integer that is invertible in F. Let $a(x) = \sum_{i=0}^{\infty} a_i x^i \in F[[x]]$ be a power series such that a_0 is a kth power in F. Show that a is a kth power in $F[[x]]$.

3. Let F be a field that is not algebraically closed. Show that $F[[x]]$ does not contain the algebraic closure of F.

4. If $a, b \in \mathbb{Z}_N$, make the definition of ab precise and show that $\mathbb{Z}_N$ is a ring.

5. Show that $\mathbb{Z}_3$ does not contain $\sqrt{-1}$. Show that $\mathbb{Z}_5$ contains two elements whose squares are -1, and compute the first 6 terms of each.

6. Use Theorem 4.4.8 to give an alternate proof that there is an injective homomorphism

$$\{f/g : f, g \in \mathbb{Z}, \gcd(g, N) = 1\} \to \mathbb{Z}_N.$$

7. Complete the details of the proof of Theorem 4.4.8, showing that all the appropriate homomorphisms commute.

8. Generalize Theorem 4.4.8 to π-adic integers. What properties of the ring R are needed to make this work?

9. Take $R = \mathbb{Z}$ and $\pi = 5$. Show that the element $5\pi^0 + 4\pi^1 + 4\pi^2 + \cdots \in \widehat{R}_\pi$ is in the kernel of $\widehat{\varphi}_n$ for all n.

10. Prove that the ring $\widehat{R}$ in Theorem 4.6.6 is an integral domain.

11. Finish the proof of Theorem 4.6.10.

12. Let R be a finite ring and let I be an ideal of R. Prove that the completion of R at I is a quotient ring of R.

13. Prove that if the continued fraction expansion of $z \in \mathbb{R}$ is eventually periodic, then z is a root of a quadratic polynomial with rational coefficients.

14. Use Hensel's lemma to determine which integers $m \in \mathbb{Z}$ have a square root in $\mathbb{Z}_p$.

15. (Reciprocal Laurent series) Let K be a field and let

$$z = \frac{x^3}{x^2 - 1} = x + x^{-1} + x^{-3} + \cdots = \sum_{i=0}^{\infty} x^{1-2i}.$$

Show that the continued fraction expansion of z is $[x, x, -x]$. That is,

$$x + x^{-1} + x^{-3} + \cdots = x + \frac{1}{x + \frac{1}{-x}}.$$

16. (Reciprocal Laurent series) Let K be a field whose characteristic is not equal to 2. Let $z^2 = (1 - x^{-1})$. Show that this equation has two solutions z in the ring $K[[x^{-1}]]$ of power series in x^{-1}. Hint: set $z = a_0 + a_1 x^{-1} + \cdots$, solve for $a_0 = \pm 1$. For $a_0 = +1$ solve recursively for a_n to find

$$0 = 2a_0 a_n + 2a_1 a_{n-1} + \cdots + \begin{cases} a_{n/2}^2 & \text{if } n \text{ is even} \\ 2a_{(n-1)/2} a_{(n+1)/2} & \text{if } n \text{ is odd.} \end{cases}$$

Do the same for $a_0 = -1$.

17. (continued) Show that the continued fraction expansion for the above z is

$$(1 - x^{-1})^{1/2} = 1 + \cfrac{1}{-2x + 1/2 + \cfrac{1}{8x - 4 + \cfrac{1}{-2x + 1 + \cfrac{1}{8x - 4 + \cfrac{1}{-2x + 1 + \cdots}}}}}$$

Bibliography

[1] M. F. Atiyah and I. G. MacDonald, *Introduction to Commutative Algebra*, Addison–Wesley, Reading MA, 1969. 22

[2] E. Bombieri and A. van der Poorten, Continued fractions of algebraic numbers, in W. Bosma and A. van der Poorten, ed., *Computational Algebra and Number Theory, Sydney, 1992*, Kluwer, 1995, pp. 137–152. 125

[3] Z. I. Borevich and I. R. Shefarevich, *Number Theory*, Academic Press: New York, N.Y., 1966. 32, 46, 76

[4] L. Carlitz and S. Uchiyama, Bounds for exponential sums, Duke Math J. **24** (1957), 37–41. 58

[5] H. Cohen, *A Course in Computational Algebraic Number Theory*, Springer Verlag, N. Y., 1993.

[6] P. Deligne, La conjecture de Weil, I, *Publ. Math. IHES* **43** (1974), 273–307. 59

[7] H. D. Ebbinghaus et al, *Numbers.* Graduate Texts in Mathematics vol. 123, Springer Verlag, N. Y. (1990).

[8] J. von zur Gathen and J. Gerhard, *Modern Computer Algebra*, second edition, Cambridge Univ. Press, Cambridge, 2003 125

[9] C. F. Gauss, *Disquisitiones Arithmeticae*, 1801; reprinted in English translation by Yale Univ. Press, New Haven, CT. 1966.

[10] S. Golomb, *Shift Register Sequences.* Aegean Park Press, Laguna Hills CA, 1982.

[11] G. Hardy and E. Wright, *An Introduction to the Theory of Numbers.* Oxford University Press, Oxford UK, 1979. 125, 129

[12] I.N. Herstein, *Topics in Algebra*, 2nd ed., 1975: Xerox College Publ., Lexington, MA.

[13] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, Springer Verlag, N.Y., 1990. 18

[14] N. Jacobson, *Basic Algebra I.* W.H. Freeman, San Francisco, 1974.

[15] N. Jacobson, *Basic Algebra II.* W.H. Freeman, San Francisco, 1980. 124

[16] A. Y. Khinchin, *Continued Fractions* (Russian), 1935. English translation: University of Chicago Press, Chicago, 1961; reprinted by Dover Publications, Mineola New York, 1997. 125, 129

[17] N. Koblitz, *p-Adic Numbers, p-Adic Analysis, and Zeta Functions,* Springer-Verlag: New York, 1984.

[18] D. Knuth, *The Art of Computer Programming, Vol 2. Seminumerical Algorithms.* Addison-Wesley, Reading MA, 1981.

[19] N. Koblitz, *p-Adic Numbers, p-Adic Analysis, and Zeta Functions.* Graduate Texts in Mathematics Vol. 58, Springer Verlag, N. Y. 1984.

[20] S. Lang, *Algebra*, 2nd ed., 1984: Addison-Wesley, Reading, MA. 11, 46, 116

[21] R. Lidl and H. Niederreiter, *Finite Fields*, 2nd ed., 1997: Cambridge University Press, Cambridge, UK. 47, 52, 58, 61, 62, 63

[22] D. Mandelbaum, A method for decoding generalized Goppa codes, *IEEE Trans. Info. Theory* **23** (1977), 137–140. 129

[23] H. Matsumura, *Commutative Algebra*, 1970: W. A. Benjamin, New York. 80

[24] B. MacDonald, *Finite Rings with Identity*, 1974: Marcel Dekker, New York. 79, 80, 81, 87, 88

[25] R. McEliece, *Finite Fields for Computer Scientists and Engineers*, 1987: Kluwer Academic Publishers, Norwell, MA.

[26] W. H. Mills, Continued fractions and linear recurrences, *Math. Comp.* **29** (1975), 173–180. 129

[27] C. D. Olds, *Continued Fractions* New Mathematical Library, Mathematical Association of America, New York, 1963 125, 129

[28] W. W. Peterson and E. J. Weldon, Jr., *Error-Correcting Codes* second edition, MIT Press, Cambridge MA, 1972.

[29] W. Schmidt, *Equations Over Finite Fields, An Elementary Approach*, Springer–Verlag, Berlin, 1976. 59

[30] B. Schneier, *Applied Cryptography.* John Wiley & Sons, New York, 1996.

[31] A. Weil, On some exponential sums, *Proc. Nat. Acad. Sci.* **34** (1948), 204–207. 59

[32] L. R. Welch and R. A. Scholtz, Continued fractions and Berlekamp's algorithm. *IEEE Trans. Info. Theory* **25** (1979), 19–27. 129

Index