1. Origins of Modern Algebra

Modern algebra was developed to solve equations.

The phrase "modern algebra" is a little vague, but it is commonly used to describe the material that appeared in van der Waerden's book *Moderne Algebra* that first appeared in 1930. Van der Waerden first encountered this material when he arrived at Göttingen in 1924. Among the primary developers of this material were Dedekind, Weber, Hilbert, Lasker, Macaulay, Steinitz, Noether, Artin, Krull, and Wedderburn, (on rings, ideals, and modules), Schur, Frobenius, Burnside, Schreier, and Galois (on groups and their representations). Van der Waerden had the advantage of attending lectures courses on algebra by Noether at Göttingen and Artin at Hamburg.

Van der Waerden's book is a marvel, as fresh today as when it was written. None of the hundreds of books covering similar ground written since casts the original into shadow.

The two basic structures of modern algebra are groups and rings.

2. From $\mathbb{N}$ to $\mathbb{Z}$ to $\mathbb{Q}$ to $\overline{\mathbb{Q}}$, $\mathbb{R}$ and $\mathbb{C}$

I disagree with the following quotation:

> Die ganze Zahl schuf der liebe Gott, alles Übrige ist Menschenwerk.
> God created the integers, all else is the work of man.
>
> *Kronecker*

Even the integers are the work of man. No doubt the first mathematical achievement of man was to recognize when two non-empty sets had the same cardinality. Then came the abstraction, picking a single label, one, two, three, et cetera, to name/describe sets having the appropriate cardinality. Thus arose the natural numbers $1, 2, 3, \ldots$.

There have been a number of primitive cultures which had no numbers beyond one, two, and three. Even cultures with more extended numbering systems have not always had a notion of zero.

The creation of the natural numbers, indeed, of all mathematics, was motivated by man's desire to understand and manipulate the world. Mathematics is a practical art.

Many equations can be solved within the integers. One can postulate simple arithmetic problems arising from everyday life that can be solved within the integers. A typical example might be *find an integer x such that $x + 27 = 30$*. At a slightly more sophisticated level, one can imagine simple division problems, such as *find x such that $3x = 60$*, that can also be solved within the positive integers. However, a mild modification, such as $3x = 67$, leads to the idea of division with remainder, and suggests how mankind was led to the rational numbers.

One can also imagine the forces that prompted the notion of negative integers.

The construction of the rationals $\mathbb{Q}$ from the integers $\mathbb{Z}$ can be formalized in such a way that a similar process applied to any domain produces its field of fractions (see section **??**). The next result summarizes the utility of the rational numbers in terms of solving certain kinds of equations. Notice that the result holds true if any field is substituted for the rationals.

Theorem 2.1. *If a, b, c are rational numbers with $a \neq 0$, then there is a unique rational number x such that $ax + b = c$.*

After linear equations come quadratics.

One of the great historical events concerning quadratics is Euclid's famous proof that $\sqrt{2}$ is not rational.

Theorem 2.2. *There is no rational number whose square is two.*

Proof. Suppose to the contrary that x is a rational number such that $x^2 = 2$. Write $x = a/b$ where a and b are integers. By cancelling common factors, we may assume that a and b have no common factor. Now, $2b^2 = a^2$, so 2 divides a^2. Hence 2 divides a, and we may write $a = 2c$. Hence $2b^2 = 4c^2$, and $b^2 = 2c^2$. It follows that b^2, and hence b, is even. Thus a and b are both divisible by 2. This contradicts the fact that a and b are relatively prime, so we conclude that 2 cannot be a square in $\mathbb{Q}$. □

This result was no doubt motivated by the problem of computing the length of the hypotenuese of the isoceles right triangle with sides of length one.

Let's focus on the proof of this result. The key point is that every non-zero element of $\mathbb{Q}$ can be written as a/b with a and b relatively prime. This fact is a consequence of a still more elementary fact, which we summarize in the next theorem.

Theorem 2.3. *Every non-zero integer can be written in an essentially unique way as a product of primes,*

$$p_1^{i_1} \cdots p_n^{i_n}$$

where $p_1, \ldots, p_n$ *are primes.*

By a prime we mean an integer p such that its only divisors are ± 1 and $\pm p$. Thus, the primes are $\{\pm 2, \pm 3, \pm 5, \cdots\}$. When we say "essentially unique" we mean that factorizations $6 = 2.3 = 3.2 = (-3).(-1).2 = 1.(-2).3.(-1)$ are to be viewed as the same; they differ only by order and the inclusion of the terms ± 1.

Two integers are relatively prime if the only numbers that divide both of them are ± 1.

This theme, the unique factorization of integers and their relatives, reappeared often in the early development of modern algebra, and it remains a staple of introductory algebra courses.

That the Greek's view of numbers and algebra was intimately connected to geometry is well documented. They had no problem accepting the existence of numbers of the form $\sqrt{d}$ with d rational because Pythagoras's theorem showed that right-angle triangles in which the lengths of two sides were rational numbers led to the conclusion that the length of the third side was of the form $\sqrt{d}$. Accepting such numbers on an (almost) equal footing with the rationals allowed the solution of a range of quadratic equations with rational coefficients.

Thus, in modern parlance, the Greeks were quite happy computing in fields such as $\mathbb{Q}(\sqrt{d})$ when d is a positive rational number.

Of course it is obvious that the equation $x^2 = -1$ has no solution in $\mathbb{Q}$, but the reason that it has no solution is quite different than the reason that $x^2 = 2$ has no solution. One can imagine that the fact that $x^2 = -1$ has no rational solution did not worry people much. It probably seemed a foolish waste of time to even consider that a problem. However, it is less apparent that an equation such as $x^2 + 2x + 2 = 0$ has no rational solution, and the discovery of this fact must surely

have been intimately related to the discovery of the general solution to a quadratic equation. Several ancient cultures independently discovered the result that

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

gives the two solutions to the quadratic equation $ax^2 + bx + c = 0$. This formula gives a criterion that the quadratic has no solution (within the reals) if $b^2 - 4ac < 0$.

This, after many centuries, led to the invention/discovery of $\sqrt{-1}$ and eventually to the notion of complex numbers. This in turn leads to the following question: *if $f(x)$ a polynomial with coefficients in a field k, is there a field K containing k in which f has a zero?* We take up this question in section 6.

Having discovered the above formula for the roots of a quadratic polynomial attention turned to the question of whether there are analogous formulas for the solutions to higher degree polynomials. Eventually, Galois gave a comprehensive solution to this problem, and we will encounter Galois theory later in this course.

Once the ancients had realized that one could pass beyond the rationals $\mathbb{Q}$ to include roots of rational numbers and more complicated expressions built from such roots, it was natural to ask if this gave "all" numbers. This question is crystallized by asking whether π is the zero of a polynomial with rational coefficients. More generally, this leads the distinction between algebraic and transcendental elements over an arbitrary field.

3. Rings

Definition 3.1. A ring is a non-empty set R endowed with two operations, addition (denoted by $+$) and multiplication,(denoted by $\times$ or $\cdot$ or juxtaposition), and satisfying for all $a, b, c \in R$:

(1) $a + b \in R$;
(2) $a + (b + c) = (a + b) + c$;
(3) $a + b = b + a$;
(4) R has a zero element, denoted 0, with the property that $0 + a = a + 0 = a$;
(5) the equation $a + x = 0$ has a solution $x \in R$; we write $-a$ for x and call it the negative of a;
(6) $ab \in R$;
(7) $a(bc) = (ab)c$;
(8) $a(b + c) = ab + bc$ and $(b + c)a = ba + ca$.

$\Diamond$

Conditions (1)-(5) say that $(R, +)$ is an abelian group with identity 0. Notice we do not call 0 the identity element, but the zero element, of R. Condition (8) connects the two different operations $+$ and $\times$. Conditions (6) and (7) are analogues of conditions (1) and (2), but there are no analogues of conditions 3, 4, and 5, for multiplication. Rings in which analogues of those conditions hold are given special names.

The smallest ring is that consisting of just one element 0; we call it the trivial ring.

One can use the distributive law to show that $0.0 = 0$ and, more generally, that $a.0 = 0$ for all $a \in R$.

Definition 3.2. We say that R is a ring with identity if there is an element $1 \in R$ such that $1.a = a.1 = a$ for all $a \in R$. We call 1 the identity element. $\Diamond$

It is easy to show that a ring can have at most one identity element.

If R is not the trivial ring and has an identity, then $1 \neq 0$; it might be easier to show that if R has an identity and $1 = 0$, then R is trivial. We will often assume that $1 \neq 0$; this simply means that $R \neq \{0\}$.

Convention. All the rings in this course will have an identity element. Most rings one encounters in algebra do have an identity. This is not so in analysis; if X is a non-compact Hausdorff space, the ring of continuous $\mathbb{R}$-valued functions on X that vanish at infinity does not have an identity.

Definition 3.3. A ring R is commutative if $ab = ba$ for all $a, b \in R$. $\Diamond$

The rings you are most familiar with, namely $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$, and $\mathbb{C}$, are commutative and have an identity. As the next example shows, many important rings are not commutative.

Example 3.4. Let S be a ring. We define $M_n(S)$, the ring of $n \times n$ matrices with entries in S as follows. As a set it consists of all matrices

$$\begin{pmatrix} s_{11} & s_{12} & \dots & s_{1n} \\ s_{21} & s_{22} & \dots & s_{2n} \\ \vdots & & & \vdots \\ s_{n1} & s_{n2} & \dots & s_{nn} \end{pmatrix}$$

where the individual entries s_{ij} are elements of S.

The addition on $M_n(S)$ is induced by that on S. If $a = (s_{ij})$ and $b = (t_{ij})$ are in $M_n(S)$, we define

$$a + b := (s_{ij} + t_{ij}),$$

the matrix whose ij^{th} entry is $s_{ij} + t_{ij}$, the sum of the ij^{th} entries of a and b.

You should check that this makes $M_n(S)$ an abelian group. Indeed, as a group, $M_n(S)$ is isomorphic to $S \times \cdots \times S$, the product of n^2 copies of S.

The multiplication in $M_n(S)$, called matrix multiplication, is defined by

$$(s_{ij}).(t_{ij}) = \left(\sum_{k=1}^{n} s_{ik} t_{kj} \right).$$

That is, the ij^{th} entry in ab is the dot product of the i^{th} row of a with the j^{th} column of b.

It is rather tedious to show that this multiplication makes $M_n(S)$ a ring. The zero element in $M_n(S)$ is the matrix with all its entries equal to zero.

If S has an identity and $S \neq 0$, then $M_n(S)$ is not commutative for $n \geq 2$; for example, if

$$a = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \qquad b = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$$

then $ab = 0 \neq ba$. $\Diamond$

Convention. All the rings in this course will be commutative. I will therefore make definitions that are appropriate for commutative rings. Whenever I say "*ring*" I mean "*commutative ring*".

Definition 3.5. Let R be a commutative ring with identity. An element $a \in R$ is called a unit if the equation $ax = 1$ has a solution in R. Such a solution is unique and is called the inverse of a and is denoted by a^{-1}. $\Diamond$

Let's check that the inverse is indeed unique: if $ab = ac = 1$, then

$$b = b.1 = b(ac) = (ba)c = (ab)c = 1.c = c.$$

Example 3.6. Let V be an infinite dimensional vector space. There are linear maps $u : V \to V$ and $v : V \to V$ such that $uv = 1$, but $vu \neq 1$. Here 1 denotes the identity map. ◊

Definition 3.7. A non-zero element a in a ring R is a zero-divisor if there is a non-zero element b such that $ab = 0$. A ring without zero-divisors is called a domain. ◊

In other words, a ring is a domain if and only if every product of non-zero elements in non-zero.

Lemma 3.8. *Let R be a commutative ring. Then R is a domain if and only if we can cancel in the following sense: whenever $0 \neq a \in R$ and $ab = ac$, then $b = c$.*

Proof. □

Recall that for any group G and any element $g \in G$, there is a unique group homomorphism $\phi : \mathbb{Z} \to G$ such that $\phi(1) = g$.

In particular, if R is a ring with identity, there is a unique group homomorphism $\phi : \mathbb{Z} \to (R, +)$ such that $\phi(1) = 1$. Warning: the two 1s in this equation are different—the first is the $1 \in \mathbb{Z}$ and the second is the $1 \in R$.

We will write n for $\phi(n)$, but of course you must then be careful when you see n to know which n you mean!

Subrings. A subring of a ring R is a subset S which is closed under addition and subtraction and multiplication, and contains 1_R.

Example 3.9. Let d be an integer that is not a square. We define

$$\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\}.$$

This is a subset of $\mathbb{C}$ and is closed under multiplication, addition, and subtraction, meaning that the product, sum, and difference, of two elements in $\mathbb{Z}[\sqrt{d}]$ belongs to $\mathbb{Z}[\sqrt{d}]$. Hence $\mathbb{Z}[\sqrt{d}]$ is a ring, a subring of $\mathbb{C}$. ◊

The product $R \times S$ of two rings. The Cartesian product

$$R \times S := \{(r, s) \mid r \in R, s \in S\}$$

of rings R and S can be given the structure of a ring by declaring

$$(r, s) + (r', s') := (r + r', s + s')$$
$$(r, s).(r', s') := (rr', ss').$$

We leave the reader to check the details. Of course, you already checked in Math 402 that $(R \times S, +)$ is an abelian group. The zero element is $(0, 0)$, and the identity is $(1, 1)$.

Some Exercises.

In all these exercises, the elements $a, b, c \ldots$ belong to a commutative ring R.

(1) Use the distributive law to show that $a.0 = 0$ for all $a \in R$.
(2) Show that a ring can have at most one identity element.
(3) Let R be a ring with identity. Show that R is the trivial ring (i.e., consists only of 0) if and only if $1 = 0$.

(4) Let R be a ring. In the abelian group $(R,+)$ we denote the inverse of a by $-a$; thus $a+(-a)=(-a)+a=0$. Of course we write $b-a$ to mean $b+(-a)$. Show that this minus sign has the following properties:
   (a) $a.(-b)=(-b).a=-(ab)$;
   (b) $(-a).(-b)=ab$;
   (c) $(-1).a=-a$.
(5) Show that a finite commutative domain is a field.
(6) Let $\phi:\mathbb{Z}\to(R,+)$ be the group homomorphism defined by $\phi(1)=1$. Show that $\phi(nm)=\phi(n)\phi(m)$ for all $n,m\in\mathbb{Z}$. Be careful when n or m is negative.
(7) Let n be a positive integer. Show that $n.a$, the product in R of n, the image of $1\in\mathbb{Z}$ under the homomorphism $\phi:\mathbb{Z}\to(R,+)$ defined by $\phi(1)=1$, is equal to $a+\cdots+a$, the sum of a with itself n times.
(8) The rings $\mathbb{Z}_p$ with p prime are NOT the only finite fields. For example, there is a field with 4 elements. Write out the addition and multiplication tables for a field with 4 elements. Denote the field by F. It must contain 0 and 1 and some element, say α, that is not equal to zero and 1. It follows that $F=\{0,1,\alpha,\alpha+1\}$—why? Write down the addition and multiplication tables, explaining how you get the entries.

4. Finite fields

Finite fields play a central role in number theory, and in applications of algebra to communications, coding theory, and several other computer-related areas.

The cyclic groups $\mathbb{Z}_n=\mathbb{Z}/n\mathbb{Z}$ may be given the structure of a ring. Just as the addition on $\mathbb{Z}$ induced the addition on $\mathbb{Z}_n$, so does the multiplication on $\mathbb{Z}$ induce a multiplication on $\mathbb{Z}_n$.

Lemma 4.1. *Let n be an integer and $\mathbb{Z}_n=\mathbb{Z}/n\mathbb{Z}$ the quotient group. Then $\mathbb{Z}_n$ becomes a commutative ring with identity $[1]$ under the multiplication defined by*

$$[a]\cdot[b]:=[ab].$$

Proof. □

We will tend to write a, or $\bar{a}$, for $[a]$, hoping that the context will always make the notation unambiguous.

Recall that the map $\phi:\mathbb{Z}\to\mathbb{Z}_n$, $\phi(a)=\bar{a}$, is a group homomorphism. It also satisfies $\phi(ab)=\phi(a)\phi(b)$; i.e., ϕ 'respects', or is 'compatible with', both the additive and multiplicative structures in $\mathbb{Z}$ and $\mathbb{Z}_n$; this says that ϕ is a ring homomorphism (see Definition 7.1 below).

Lemma 4.2. *Let a and n be integers. Then $(a,n)=1$ if and only if the equation $ax=1$ has a solution in $\mathbb{Z}_n$.*

Proof. □

Theorem 4.3. *$\mathbb{Z}_n$ is a field if and only if n is prime.*

Proof. ($\Leftarrow$) If n is prime and $0\neq[a]\in\mathbb{Z}_n$, then n does not divide a, so $(a,n)=1$. By Lemma 4.2, there is an element $x\in\mathbb{Z}_n$ such that $ax=1$. Hence $\mathbb{Z}_n$ is a field.

($\Rightarrow$) We will prove this by contradiction. Suppose n is not prime. Then $n=ab$ with $\{a,b\}\cap\{1,-1\}=\phi$. In particular, n does not divide a, so a is a non-zero

element of $\mathbb{Z}_n$. If a had an inverse, say $xa = 1$, in $\mathbb{Z}_n$, then we would have the following in $\mathbb{Z}_n$:

$$b = 1.b = (xa)b = x(ab) = 0.$$

But this implies that n divides b, whence a must be ± 1; this is a contradiction, so we conclude that a cannot have an inverse in $\mathbb{Z}_n$. □

Notation. If p is a positive prime integer, we write $\mathbb{F}_p$ for the field with p elements. In other words, $\mathbb{F}_p = \mathbb{Z}_p$. Later on we shall see that there is a finite field with p^n elements and we will denote this by $\mathbb{F}_{p^n}$. These are all the finite fields.

Inverses in $\mathbb{F}_p$. Consider the problem of explicitly finding the inverse of an element in $\mathbb{F}_p$. For example, what is the inverse of 13 in $\mathbb{F}_{19}$? Since 19 is prime, the greatest common divisor of 13 and 19 is 1, and there are integers a and b such that $1 = 13a + 19b$. The image of a in $\mathbb{F}_{19}$ is the inverse of 13. To find a and b we apply the Euclidean algorithm to get

$$19 = 1 \times 13 + 6, \qquad 13 = 2 \times 6 + 1,$$

so

$$1 = 13 - 2 \times 6 = 13 - 2 \times (19 - 13) = 3 \times 13 - 2 \times 19.$$

Hence $13^{-1} = 3$ in $\mathbb{F}_{19}$. Check that $13 \times 3 = 39 = 2 \times 19 + 1$.

5. Other Fields

It would be foolish to develop a theory of fields if those in Theorem 4.3 were the only examples. Fields abound. The simplest examples beyond those you already know are those in the next example.

Example 5.1. Let d be a rational number that it is not a square in $\mathbb{Q}$. The subset

$$\mathbb{Q}(\sqrt{d}) := \{a + b\sqrt{d} \mid a, b \in \mathbb{Q}\}$$

of $\mathbb{C}$ is closed under multiplication and addition, meaning that the product and sum of two in $\mathbb{Q}(\sqrt{d})$ belong to $\mathbb{Q}(\sqrt{d})$, so is a subring of $\mathbb{C}$. The inverse (in $\mathbb{C}$) of a non-zero element of $\mathbb{Q}(\sqrt{d})$ belongs to $\mathbb{Q}(\sqrt{d})$, namely

$$\big(a + b\sqrt{d}\big)^{-1} = \frac{a}{a^2 - b^2 d} - \frac{b}{a^2 - b^2 d}\sqrt{d};$$

the denominator is non-zero because d is not a square in $\mathbb{Q}$. Thus $\mathbb{Q}(\sqrt{d})$ is a field. ◊

Exercise. Let n be a positive integer and $\zeta = e^{2\pi i/n}$. Show that

$$\mathbb{Q}(\zeta) := \{a_0 + a_1\zeta + \cdots + a_{n-1}\zeta^{n-1} \mid a_0, \ldots, a_{n-1} \in \mathbb{Q}\}$$

is a subfield of $\mathbb{C}$.

Exercise. Think of six interesting questions about the fields $\mathbb{F}_p$, $\mathbb{Q}(\sqrt{d})$, and $\mathbb{Q}(\zeta)$.

Later, we will examine fields in some detail, but for now we simply introduce them as a necessary preliminary for our discussion of polynomials. Fields provide the coefficients for polynomials.

The letter k is often used to denote a field because German mathematicians, who were the first to examine fields in some detail, called a field *ein körper* (körper=body, cf. "corpse"). Despite this nomenclature, the study of fields remains a lively topic.

There are finite fields $\mathbb{F}_{p^n}$ with p^n elements for every prime p and every integer $n \geq 1$. Here, for example, is how to construct $\mathbb{F}_4$ with your bare hands.

Construction of $\mathbb{F}_4$. First, $\mathbb{F}_4$ contains a zero and an identity and, because it has four elements, an element different from both zero and one that we will call α.

We can add in $\mathbb{F}_4$, so $\mathbb{F}_4$ contains an element $\alpha + 1$. We will now show that $\alpha + 1 \notin \{0, 1, \alpha\}$. To do this we first show that $1 + 1 = 0$ in $\mathbb{F}_4$. To see this, observe that $(\mathbb{F}_4, +)$ is a group with four elements, so every element in it has order dividing 4; in particular,

$$0 = 1 + 1 + 1 + 1 = (1 + 1).(1 + 1) = (1 + 1)^2,$$

but $\mathbb{F}_4$ is a field, so $1 + 1 = 0$. We can also write this as $-1 = 1$ in $\mathbb{F}_4$.

If $\alpha + 1 = 0$, then adding 1 to both sides gives $\alpha = 1$, a contradiction; if $\alpha + 1 = 1$, then adding 1 to both sides gives $\alpha = 0$, a contradiction; if $\alpha + 1 = \alpha$, then subtracting α from both sides gives $1 = 0$, a contradiction. We conclude that $\alpha + 1 \notin \{0, 1, \alpha\}$, and hence

$$\mathbb{F}_4 = \{0, 1, \alpha, \alpha + 1\}.$$

We have already done most of the work to construct the addition table; the only other calculation that needs to be done is

$$\alpha + \alpha = 1.\alpha + 1.\alpha = (1 + 1).\alpha = 0.\alpha = 0.$$

The essential calculation needed to construct the multiplication table for $\mathbb{F}_4$ is to determine α^2. Since $\mathbb{F}_4$ is a field $\alpha^2 \neq 0$. If $\alpha^2 = 1$, then

$$0 = \alpha^2 - 1 = (\alpha + 1)(\alpha - 1) = (\alpha + 1)(\alpha + 1),$$

and this cannot happen because $\mathbb{F}_4$ is a domain and $\alpha + 1$ is not zero. If $\alpha^2 = \alpha$, then

$$0 = \alpha^2 - \alpha = \alpha(\alpha - 1) = \alpha(\alpha + 1),$$

and this cannot happen because $\mathbb{F}_4$ is a domain. The only possibility is that $a^2 = \alpha + 1$. It is now easy to write out the multiplication table.

6. The polynomial ring in one variable

Throughout this section k denotes a field.

Let R be a commutative ring. To begin with you might think of R being the integers, or the rationals, the reals, or some other field you know and love. Polynomials in one variable, say x, with coefficients in R can be added and multiplied in the obvious way to produce another polynomial with coefficients in R.

We write $R[x]$ for the set of all polynomials in x with coefficients in R. An element of $R[x]$ is an expression

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$$

where the coefficients a_i belong to R. Addition and multiplication are defined in the obvious way. Two polynomials are considered to be the same only if all their coefficients are the same. In this way $R[x]$ becomes a ring, with zero element the zero polynomial 0, and identity element the constant polynomial 1.

Definition 6.1. Let R be a ring. The polynomial ring with coefficients in R, which we denote by $R[x]$, consists of all formal expressions

$$\alpha_0 + \alpha_1 x + \alpha_2 x^2 + \ldots + \alpha_n x^n$$

where $\alpha_0, \ldots, \alpha_n \in R$, and this is made into a ring by defining the sum and product of two polynomials by

$$\sum \alpha_i x^i + \sum \beta_i x^i := \sum (\alpha_i + \beta_i) x^i$$

and

$$\left(\sum \alpha_i x^i\right)\left(\sum \beta_i x^i\right) := \sum_n \left(\sum_{j=0}^{n} (\alpha_j \beta_{n-j}\right) x^n.$$

We call $\alpha_0, \ldots, \alpha_n$ the coefficients of $\sum_{i=0}^{n} \alpha_i x^i$. We say that two polynomials are equal if and only if they have the same coefficients.

We call x an indeterminate. ◊

We leave it to the reader to check that $R[x]$ is a ring.

We are particularly interested in the case when R is a field.

The ring of polynomials in one variable with coefficients in a field behaves in many respects like the ring of integers. We will see this when we consider questions of division and factorization.

Recall that if a and b are integers with b non-zero, then there are integers q and r such that $a = bq + r$ and $0 \leq r < |b|$. We usually call r the remainder. This result plays a key role in arithmetic. To show that there is an analogous result for $k[x]$ we need a notion of "size" to replace absolute value.

The degree of a non-zero element $f = a_n x^n + \cdots + a_1 x + a_0$ in $R[x]$ is n provided that $a_n \neq 0$. In that case we call a_n the leading coefficient of f. If $f = 0$ it is convenient to define its degree to be $-\infty$. It is a trivial observation that the units in $k[x]$ are precisely the polynomials of degree zero.

Lemma 6.2. *Let R be a domain and let $f, g \in R[x]$. Then*

(1) $\deg(f + g) \leq \max\{\deg f, \deg g\}$;
(2) $\deg(fg) = \deg f + \deg g$;
(3) $R[x]$ *is a domain.*

More variables. It is clear that we can jazz up this definition and define for any positive integer n the polynomial ring in n variables, $k[x_1, \ldots, x_n]$. The rings $k[x, y]$ and $k[x, y, z]$, or perhaps $\mathbb{R}[x, y]$ and $\mathbb{R}[x, y, z]$, should not cause too much fear. Just add and multiply polynomials in the way you have been doing for years.

7. Ring homomorphisms and ideals

As with any collection of mathematical objects, we must specify the allowable maps $R \to S$ between two rings. These are the ring homomorphisms. Roughly, a ring homomorphism is a map between rings that "respects" the addition and multiplication operations in them. We also have a notion of kernel (those elements sent to zero) and image; the kernel of a homomorphism has certain properties which lead to the definition of a two-sided ideal—the kernel is a two-sided ideal. The image of a homomorphism $f : R \to S$ is itself a ring, a subring of S, and there is an isomorphism $R/\ker f \cong \mathrm{im}(f)$. We have the notion of an ideal "generated" by a set of elements (the smallest ideal containing those elements, and this makes sense because an intersection of ideals is an ideal); and we also have the notion of the subring generated by a set of elements, which is the smallest subring containing them.

Definition 7.1. A homomorphism $f : R \to S$ of rings is a map such that $f(xy) = f(x)f(y)$ and $f(x + y) = f(x) + f(y)$ for all $x, y \in R$, and $f(1_R) = 1_S$. If f is a bijective ring homomorphism we call it an isomorphism, and say that R is isomorphic to S, and denote this by $R \cong S$. In this case f^{-1} is a ring homomorphism too. $\Diamond$

The image of a ring homomorphism $\phi : R \to S$ is a subring of S.

If R is a subring of a ring S the inclusion $R \to S$ is a ring homomorphism. For example, the inclusions $\mathbb{Z} \to \mathbb{Q} \to \mathbb{R} \to \mathbb{C} \to \mathbb{C}[x]$ are all ring homomorphisms.

A composition of ring homomorphisms is a ring homomorphism.

Example 7.2. If R is any ring with identity there is a unique ring homomorphism $\phi : \mathbb{Z} \to R$. We must have $\phi(1) = 1$ because that is a requirement of *every* ring homomorphism; it follows that if n is a positive integer, then

$$\phi(n) = \phi(1 + \cdots + 1) = \phi(1) + \cdots + \phi(1) = 1 + \cdots + 1 = n,$$

where there are n terms in each of these sums, and $0 = \phi(n - n) = \phi(n) + \phi(-n) = n + \phi(-n)$, so $\phi(-n) = -n$. Notice that we have taken the liberty of writing n for the element in R that is the sum of 1_R with itself n times. Hopefully, this will not cause confusion! Of course, ϕ sends $-n$ to $(-1) + (-1) + \cdots + (-1)$, the sum of -1 taken n times. Hence if $x \in R$ and $n \in \mathbb{Z}$ we often write nx for $x + \cdots + x$, the sum of x taken n times (if $n \geq 0$); this is the product of x and n, where n is viewed as an element of R via ϕ. $\Diamond$

You have been working with polynomials for many years: when you plug a value into a polynomial you are applying a homomorphism.

Example 7.3. Let k be a field and R a larger commutative ring containing k. Fix some element $\lambda \in R$. Then each polynomial in $k[x]$ can be evaluated at λ, by plugging in λ; that is, every time you see x replace it by λ and then evaluate the resulting expression in R to get an element $f(\lambda)$ in R.

The rule $\varepsilon : k[x] \to R$ defined by

$$\varepsilon(f) = f(\lambda)$$

is a ring homomorphism. Explicitly, if $f(x) = \alpha_0 + \alpha_1 x + \cdots + \alpha_n x^n$, then

$$\varepsilon(f) = f(\lambda) = \alpha_0 + \alpha_1 \lambda + \cdots + \alpha_n \lambda^n.$$

You should check that ε is a ring homomorphism: this is very easy because it simply says something you have known for may years, namely $(f+g)(\lambda) = f(\lambda)+g(\lambda)$ and $(fg)(\lambda) = f(\lambda)g(\lambda)$. All this is no accident; evaluating polynomials had been going on for many centuries before the abstract notions of rings and homomorphisms were introduced, and those notions were introduced so as to formalize and make precise what had long been going on. $\Diamond$

The image of the homomorphism $\varepsilon : k[x] \to R$ is denoted by $k[\lambda]$.

Example 7.4. Complex conjugation, $z \mapsto \bar{z}$, is an isomorphism $\phi : \mathbb{C} \to \mathbb{C}$. When you first met complex conjugation you will have checked that $\overline{wz} = \bar{w}\bar{z}$ and $\overline{w + z} = \bar{w} + \bar{z}$. In other words, you checked then that complex conjugation is a ring homomorphism. $\Diamond$

Example 7.5. The map $\phi : \mathbb{F}_4 \to \mathbb{F}_4$ defined by $\phi(\alpha) = \alpha + 1$ is a ring homomorphism. You should check this by using the addition and multiplication tables for $\mathbb{F}_4$. $\Diamond$

Remark. When defining a ring homomorphism $\phi : R \to S$, we are often lazy: we don't always give an explicit formula for $\phi(r)$ for every $r \in R$. For example, we might define $\phi : \mathbb{Q}[x] \to \mathbb{R}$ by saying that ϕ is the ring homomorphism defined by $\phi(x) = \sqrt{7}$. What we are really saying is that there is a unique ring homomorphism $\phi : \mathbb{Q}[x] \to \mathbb{R}$ such that $\phi(x) = \sqrt{7}$, and that it is then routine to figure out what $\phi(f)$ is for every $f \in \mathbb{Q}[x]$.

Because ϕ is a ring homomorphism, $\phi(\alpha_0 + \alpha_1 x + \cdots + \alpha_n x^n)$ must equal

$$\phi(\alpha_0) + \phi(\alpha_1)\phi(x) + \cdots + \phi(\alpha_n)\phi(x)^n.$$

Now, $\phi(x)^i = (\sqrt{7})^i$, so we only need to know what $\phi(\alpha)$ is for $\alpha \in \mathbb{Q}$. The restriction of ϕ to $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{Q}[x]$ is a ring homomorphism $\mathbb{Z} \to \mathbb{R}$; but, as discussed in Example 7.2, there is only one ring homomorphism $\mathbb{Z} \to \mathbb{R}$, and this is the inclusion. Thus $\phi(n) = n$ for all $n \in \mathbb{Z}$. If n is a non-zero integer, then

$$1 = \phi(1) = \phi(n.n^{-1}) = n.\phi(n^{-1}),$$

so $\phi(n^{-1}) = n^{-1}$, and $\phi(m/n) = \phi(m)\phi(n^{-1}) = mn^{-1}$, so

$$\phi(\alpha_0 + \alpha_1 x + \cdots + \alpha_n x^n) = \alpha_0 + \alpha_1\sqrt{7} + \cdots + \alpha_n(\sqrt{7})^n.$$

The same sort of laziness is employed in defining the homomorphism ϕ in Example 7.4.

Example 7.6. If m and n are relatively prime positive integers, there is an isomorphism of rings

$$\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n.$$

To see this, define $\phi : \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n$ by

$$\phi[a + (mn)] = \big([a + (m)], [a + (n)]\big).$$

First, ϕ is well-defined because if $[a+(mn)] = [b+(mn)]$, then $a-b$ is a multiple of mn, hence a multiple of both m and n, so $[a+(m)] = [b+(m)]$ and $[a+(n)] = [b+(n)]$. It is easy to check that ϕ is a ring homomorphism (you should do it even/especially if I don't). We now claim that ϕ is an isomorphism; to check this we must show it is bijective. Both $\mathbb{Z}_{mn}$ and $\mathbb{Z}_m \times \mathbb{Z}_n$ have mn elements, so it suffices to show that ϕ is injective. If $\phi[a+(mn)] = \phi[b+(mn)]$, then $a-b$ is divisible by both m and n, and hence by their product because $\gcd(m, n) = 1$; it follows that $[a+(m)] = [b+(m)]$, thus showing that ϕ is injective and hence an isomorphism. ♢

7.1. **Ideals.**

Definition 7.7. An ideal of a ring R is a subset I which is a subgroup under $+$, and contains ar whenever $r \in R$ and $a \in I$.

If A is a subset of R we define the ideal, generated by A as the smallest ideal containing A. ♢

Notation. Let $a \in R$. The ideal generated by a is

$$Ra := \{ra \mid r \in R\}.$$

We call Ra the principal ideal generated by a, and sometimes denote it by (a).

It is easy to verify that the ideal generated by $a_1, \cdots, a_n \in R$ is

$$Ra_1 + \cdots + Ra_n := \{r_1a_1 + \cdots + r_na_n \mid r_1, \ldots, r_n \in R\}.$$

We sometimes denote this ideal by $(a_1, \ldots, a_n)$.

Basic results. The ring R itself is an ideal, and so is $0 = \{0\}$.

If an ideal I contains a unit, say u, then $I = R$ because if $r \in R$, then $r = u.u^{-1}r$ is a multiple of an element in I so belongs to I. It follows that the only ideals of a field are the zero ideal and the field itself. The converse is also true: if R has no ideals other than zero and itself and $0 \neq u \in R$, then uR is an ideal so must equal R, whence $1 = uv$ for some $v \in R$, so u is a unit.

You should check that if I and J are ideals, so is their intersection $I \cap J$, and their sum

$$I + J := \{i + j \mid i \in I,\ j \in J\},$$

and their product

$$IJ := \{i_1 j_1 + \cdots + i_n j_n \mid i_1, \ldots, i_n \in I,\ j_1, \ldots, j_n \in J\}.$$

Definition 7.8. Let $\phi : R \to S$ be a ring homomorphism. The kernel of ϕ is

$$\ker \phi := \{a \in R \mid \phi(a) = 0\}.$$

$\Diamond$

Proposition 7.9. *The kernel of a ring homomorphism $\phi : R \to S$ is an ideal of R.*

Proof. Since ϕ is a group homomorphism $(R, +) \to (S, +)$, $\ker \phi$ is certainly a subgroup of $(R, +)$. Moreover if $a \in \ker \phi$ and $r \in R$, then $\phi(ar) = \phi(a)\phi(r)$ and this is zero because $\phi(a) = 0$. $\square$

Exercise: A ring homomorphism $\phi : R \to S$ is injective if and only if $\ker \phi = \{0\}$.

The quotient by an ideal. If I is a two-sided ideal of R, we write R/I for the set of cosets

$$[x + I] := \{x + a \mid a \in I\}.$$

Thus R/I has the same meaning as it did in group theory, and R/I becomes an abelian group under the induced addition. In fact, R/I can be given the structure of a ring by defining

$$[x + I] + [y + I] := [x + y + I] \qquad \text{and} \qquad [x + I].[y + I] := [xy + I],$$

for all $x, y \in R$. One must check that these definitions are unambiguous, and that they do make R/I a ring. The zero element in R/I is $[0 + I] = I$, and the identity is $[1 + I]$. If R is commutative, so is R/I.

Proposition 7.10. *The map $R \to R/I$ defined by $x \mapsto [x + I]$ is a surjective ring homomorphism with kernel I.*

Proof. Left to the reader. This is easy, but you should prove it once in your life in order to understand why it is easy! The point is to see how the definition of addition and multiplication in R/I synchronizes with the axioms for a map to be a ring homomorphism. $\square$

We will make frequent use of the previous result, and especially its companion, Proposition 7.11 below, which applies this result to quotients of polynomial rings.

Let k be a field and I an ideal of $k[x]$. Suppose that $I \neq k[x]$, so $k[x]/I$ is not the zero ring. The inclusion $k \to k[x]$ composed with the homomorphism $k[x] \to k[x]/I$, $a \mapsto [a + I]$, gives a homomorphism $\psi : k \to k[x]/I$. Since $I \cap k = \{0\}$, the kernel of ψ is zero, whence ψ is injective. Because the map $\psi : k \to k[x]/I$ is injective

we may identify k with its image in $k[x]/I$. We often do this. For example, this is what we do in the next result: to make sense of the statement of Proposition 7.11 we must view k as a subring of $k[x]/(f)$.

Proposition 7.11. *Let k be a field and $f \in k[x]$ be a polynomial of degree $n \geq 1$. Write $\bar{x}$ for $[x + (f)]$, the coset containing x and view $\bar{x}$ as an element of $k[x]/(f)$. Then every element of $k[x]/(f)$ can be written as*

$$\lambda_0 + \lambda_1\bar{x} + \cdots + \lambda_{n-1}\bar{x}^{n-1}$$

for unique elements $\lambda_1, \lambda_1, \ldots, \lambda_{n-1} \in k$.

Proof. We need to use Proposition 11.1 to prove this: given $g \in k[x]$ we can write $g = qf + r$ for some $q, r \in k[x]$ with $\deg r < n$. You can either take this on faith or look ahead to page 23.

Obviously $[g + (f)] = [r + (f)]$, so

$$k[x]/(f) = \{[g + (f)] \mid g \in k[x]\} = \{[r + (f)] \mid \deg r < n\}.$$

If $r = \lambda_0 + \lambda_1 x + \cdots + \lambda_{n-1}x^{n-1}$, then

$$\begin{aligned}[r + (f)] &= [\lambda_0 + \lambda_1 x + \cdots + \lambda_{n-1}x^{n-1} + (f)] \\ &= [\lambda_0 + (f) + [\lambda_1 + (f)][x + (f)] + \cdots + [\lambda_{n-1} + (f)][x + (f)]^{n-1} \\ &= \lambda_0 + \lambda_1\bar{x} + \cdots + \lambda_{n-1}\bar{x}^{n-1}\end{aligned}$$

The uniqueness is because if

$$\lambda_0 + \lambda_1\bar{x} + \cdots + \lambda_{n-1}\bar{x}^{n-1} = \mu_0 + \mu_1\bar{x} + \cdots + \mu_{n-1}\bar{x}^{n-1}$$

then $(\lambda_0 - \mu_0) + (\lambda_1 - \mu_1)x + \cdots + (\lambda_{n-1} - \mu_{n-1})x^{n-1}$ is in (f). But the only polynomial of degree $< n$ that is a multiple of f is the zero polynomial. □

Proposition 7.12. *Let $\phi : S \to R$ be a ring homomophism. There is an isomorphism of rings*

$$S/\ker\phi \cong \mathrm{im}(\phi).$$

Proof. Write $I = \ker\phi$. Since ϕ is a group homomorphism, the proof of the analogous result for groups already shows that the map $\theta : R/I \to \mathrm{im}\,\phi$ defined by $\theta([x + I]) = \phi(x)$ is an isomorphism of abelian groups. So all that remains is to check that $\theta(x)\theta(y) = \theta(xy)$, but this follows at once from the definition of multiplication in R/I. □

Exercise. Let $\theta : R \to S$ be a ring homomorphism and I an ideal of R such that $\theta(I) = 0$. Let $\pi : R \to R/I$ be the natural map. Show there is a unique homomorphism $\phi : R/I \to S$ such that $\theta = \phi\pi$.

Example 7.13. If $\lambda \in k$, then $k[x]/(x - \lambda) \cong k$. To see this, let $\phi : k[x] \to k$ be the homomorphism given by plugging in λ; that is, $\phi(f) = f(\lambda)$. Clearly ϕ is surjective—if $\alpha \in k$, then $\alpha = \phi(\alpha)$! If f is a multiple of $x - \lambda$, then $\phi(f) = 0$, so $\ker\phi \supset (x - \lambda)$. However, a polynomial f can be written as $f = (x - \lambda)q + f(\lambda)$ for a suitable $q \in k[x]$, so we see that $\phi(f) \neq 0$ if f is not a multiple of $x - \lambda$. Hence $\ker\phi = (x - \lambda)$. The isomorphism $k[x]/(x - \lambda) \cong k$ now follows from Proposition 7.12. ◊

The kernel of a homomorphism $\phi : R \to S$ provides a precise measure of the (lack of) injectivity of ϕ—ϕ is injective if and only if $\ker \phi = \{0\}$; more explicitly, since $\phi(a) = \phi(b)$ if and only if $a - b \in \ker \phi$, one sees that $\phi(a) = \phi(b)$ if and only if $[a + \ker \phi] = [b + \ker \phi]$. It follows that the fibers of ϕ, that is the subsets

$$\phi^{-1}(s) := \{r \in R \mid \phi(r) = s\} \subset R, \qquad s \in S,$$

are either empty or cosets of $\ker \phi$.

Lemma 7.14. *If J is an ideal in R containing an ideal I, then J/I is an ideal of R/I and every ideal of R/I is obtained in this way.*

Proof. See the homework exercises on page 22. □

7.2. **Maximal ideals and fields.**

Lemma 7.15. *Let $u \in R$. Then u is a unit if and only if $(u) = R$.*

Proof. ($\Rightarrow$) If u is a unit, there is an element $v \in R$ such that $1 = uv$; thus $r = uvr$ for $r \in R$; in other words, every element of R is a multiple of u, which says that $R = (u)$.

($\Leftarrow$) If $R = (u)$, then every element of R is a multiple of u. In particular, 1 is, so $1 = uv$ for some $v \in R$, thus showing that v is a unit. □

Lemma 7.16. *A commutative ring R is a field if and only if its only ideals are* 0 *and R itself.*

Proof. ($\Rightarrow$) If I is a non-zero ideal of R it contains a non-zero element, say u. But u is a unit by the hypothesis, so $r = ruu^{-1} \in I$ for every $r \in R$. That is, $I = R$.

($\Leftarrow$) Let u be a non-zero element of R. Then the ideal (u) is non-zero, so is equal to R by hypothesis; Lemma 7.15 now implies that u is a unit. □

An ideal I in a ring R is maximal if the only ideal that contains I but is not equal to it is R itself.

One sees easily that $(x - \lambda)$ is a maximal ideal of $k[x]$, but in general there will be other maximal ideals—that is the case when k is not algebraically closed (see below).

Lemma 7.17. *An ideal I in a ring R is maximal if and only if R/I is a field.*

Proof. This follows immediately from Lemma 7.14, but here is an alternative proof.

Suppose that I is maximal. A non-zero element of R/I can be written as $[a + I]$ for some $a \notin I$. Since I is maximal $aR + I = R$. Hence there are elements $b \in R$ and $c \in I$ such that $1 = ab + c$. In R/I,

$$[a + I][b + I] = [ab + I] = [1 - c + I] = [1 + I] = 1_{R/I}.$$

Hence $[b + I]$ is the inverse in R/I of $[a + I]$. This shows that R/I is a field.

Conversely, suppose that R/I is a field. Let J be an ideal of R that is strictly larger than I. There is an element $a \in J \backslash I$. Since $[a + I]$ is a non-zero element of R/I, it has an inverse, say $[b + I]$. Since

$$1_{R/I} = [1 + I] = [a + I][b + I] = [ab + I],$$

$1 - ab \in I$, and $1 \in aR + I \subset J$. Hence $J = R$, showing that I is maximal. □

Example 7.18. $\mathbb{R}[x]/(x^2 + 1) \cong \mathbb{C}$. ◊

7.3. **Ideals in $\mathbb{Z}$.**

Proposition 7.19. *The ideals in $\mathbb{Z}$ are $n\mathbb{Z}$, $n \geq 0$.*

Proof. First observe that each $n\mathbb{Z}$ is an ideal of $\mathbb{Z}$. On the other hand, we showed in Math 402 that the only subgroups of $(\mathbb{Z}, +)$ are the various $n\mathbb{Z}$, and since an ideal is first a subgroup, the result follows. □

Here is a cute observation regarding the notation (a, b) in the ring $\mathbb{Z}$. We use this notation for two different things: it denotes the ideal generated by a and b, namely $a\mathbb{Z} + b\mathbb{Z}$, and it denotes the greatest common divisor of a and b. Now Proposition 7.19 tells us that the ideal (a, b) is equal to $d\mathbb{Z}$, or (d), for some integer d; it turns out that we can take d to be the greatest common divisor of a and b so the two notations have (almost) the same meaning after all.

To prove this claim, let d denote the gcd of two non-zero integers a and b. To see that $(a, b) = (d)$ notice first that $(a) \subset (d)$ because $d|a$ and $(b) \subset (d)$ because $d|b$ so, as ideals are closed under $+$, $(d) \supset (a) + (b) = (a, b)$. The reverse inclusion also holds because there are integers u and v such that $d = au + bv$, and hence $d \in (a, b)$ and hence $(d) \subset (a, b)$.

8. Some examples

There is nothing difficult about the examples in this section. Mostly it is a matter of becoming familiar with the notation, and ideas, and that does take some time. Practice, practice, practice!

The ideal (x^3+1, x^2-2) in $\mathbb{Q}[x]$ is equal to $\mathbb{Q}[x]$. Write $I = (x^3+1, x^2-2)$. Recall that (a, b) denotes the ideal of a ring R consisting of the elements $\{ar + bs \mid r, s \in R\}$. Dividing $x^3 + 1$ by $x^2 - 2$ and finding the remainder gives

$$x^3 + 1 = x(x^2 - 2) + 2x + 1,$$

which can be rewritten as $2x + 1 = (x^3 + 1).1 + (x^2 - 2).(-x)$, so $2x + 1 \in I$. Dividing $x^2 - 2$ by $2x + 1$ and finding the remainder gives

$$x^2 - 2 = (2x + 1)\tfrac{1}{4}(2x - 1) - \tfrac{7}{4},$$

from which it follows that $\frac{7}{4} \in I$, and hence $\frac{7}{4}.\frac{4}{7} = 1 \in I$. But once $1 \in I$, so is $r.1$ for every $r \in \mathbb{Q}[x]$, so $I = \mathbb{Q}[x]$.

There is an isomorphism of rings $\mathbb{C}[x]/(x^2 - 1) \cong \mathbb{C} \times \mathbb{C}$. Almost always when one wants to establish an isomorphism of the form $S/I \cong R$, one does so by finding a surjective ring homomorphism $\phi : S \to R$ such that $\ker \phi = I$ and then invoking Proposition 7.12. That is what we do here.

Define $\phi : \mathbb{C}[x] \to \mathbb{C} \times \mathbb{C}$ by

$$\phi(f) := (f(1), f(-1)).$$

It is elementary to show that ϕ is a homomorphism: recall from Example 7.3 that "plugging in" is a ring homomorphism; you should check this! To see that ϕ is surjective observe that

$$(\alpha, \beta) = \phi\left(\tfrac{1}{2}\alpha(x + 1) - \tfrac{1}{2}\beta(x - 1)\right).$$

Now

$$f \in \ker \phi \Leftrightarrow 0 = \phi(f) \Leftrightarrow f(1) = f(-1) = 0 \Leftrightarrow x^2 - 1 \text{ divides } f,$$

so $\ker f = (x^2 - 1)$.

The same sort of argument will show that $\mathbb{R}[x]/(x^2-1) \cong \mathbb{R} \times \mathbb{R}$ and $\mathbb{Q}[x]/(x^2 - 1) \cong \mathbb{Q} \times \mathbb{Q}$. However, the argument would not show that $\mathbb{Z}[x]/(x^2-1)$ is isomorphic to $\mathbb{Z} \times \mathbb{Z}$, so let's ask the question: is $\mathbb{Z}[x]/(x^2 - 1)$ isomorphic to $\mathbb{Z} \times \mathbb{Z}$? Hint: the element $f = (1, 0)$ in $\mathbb{Z} \times \mathbb{Z}$ satisfies $f^2 = f$; is there an element in $\mathbb{Z}[x]/(x^2 - 1)$ that is equal to its own square?

If $d \in \mathbb{Q}$ is not a square, then $\mathbb{Q}[x]/(x^2 - d) \cong \mathbb{Q}(\sqrt{d})$. Define $\phi : \mathbb{Q}[x] \to \mathbb{Q}(\sqrt{d})$ by $\phi(f) := f(\sqrt{d})$. This is surjective (why?) and has kernel equal to (x^2-d) (why?).

$\mathbb{R}[x]/(x^2 + x + 3) \cong \mathbb{C}$ To prove this by invoking Proposition 7.12 we first need a homomorphism $\phi : \mathbb{R}[x] \to \mathbb{C}$ whose kernel is $(x^2 + x + 3)$. If we write $a = \phi(x)$, then a must satisfy $a^2 + a + 3 = \phi(x^2 + x + 3) = 0$ in $\mathbb{C}$. So, let a be one of the complex zeroes of $x^2 + x + 3$ and define ϕ by

$$\phi(f) = f(a).$$

Then $\ker \phi = (x^2 + x + 3)$ as required.

$\mathbb{F}_2[x]/(x^2 + x + 1) \cong \mathbb{F}_4$

Some Exercises.

In all these exercises, the elements $a, b, c \ldots$ belong to a commutative ring R.

(1) If $a = bc + d$ show that $(a, c) = (d, c)$.
(2) Show that $\mathbb{Z}[x]/(x) \cong \mathbb{Z}$. (Hint: in this and the next exercise, use Proposition 7.12.)
(3) Show that $\mathbb{Z}[x]/(n) \cong \mathbb{Z}_n[x]$ for every integer $n > 0$.
(4) We define a I of $\mathbb{Z}[x]$ as follows: f is in I if and only if the sum of its coefficients is zero. Show that I is an ideal in two ways: first, by using the definition of an ideal; second, by exhibiting I as the kernel of a homomorphism. Which method is easier?
(5) Find generators for the ideal I in the previous question.
(6) We define a I of $\mathbb{Z}[x]$ as follows: f is in I if and only if the constant term of I is a multiple of 8. Show that I is an ideal in two ways: first, by using the definition of an ideal; second, by exhibiting I as the kernel of a homomorphism. Which method is easier?
(7) Find generators for the ideal I in the previous question.
(8) Let X be any set and k any field. Show that the set S of all functions $X \to k$ can be made into a ring in an obvious way—use the addition and multiplication in k to define addition and multiplication in S.
(9) Think of the elements of $\mathbb{R}[x, y]$, the ring of polynomials with real coefficients, as functions $\mathbb{R}^2 \to \mathbb{R}$. That is, $f(x, y)$ evaluated at the point (a, b) in the real plane is $f(a, b) \in \mathbb{R}$. Let C be the curve $y^2 = x(x^2 - 1)$ in $\mathbb{R}^2$. By restricting $f \in \mathbb{R}[x, y]$ to $C \subset \mathbb{R}^2$ we get a map $\phi : \mathbb{R}[x, y] \to S$ where S is the ring of all functions $C \to \mathbb{R}$. Show that ϕ is a ring homomorphism, and determine its kernel.
(10) Show that $x^8 + xz^7 + x^6 + x^4 + 1$ divides $x^{15} - 1$ in $\mathbb{F}_2[x]$.

9. Arithmetic in $\mathbb{Z}$

After learning to count and add, children learn how to multiply and divide. Questions about division and factorization are of primary importance in all rings. We begin here with $\mathbb{Z}$.

Recall that an integer p is prime if the only numbers dividing it are ± 1 and $\pm p$.

If an integer m divides an integer m we write $n|m$.

Lemma 9.1. *Let n be an integer ≥ 2. Then n has a positive prime divisor.*

Proof. Let $\Phi = \{m > 1 \mid m|n\}$. Then $\Phi \subset \{2, \dots, n\}$, so has a smallest element, say p. Certainly p divides n. If p were not prime there would be a positive integer q dividing p and satisfying $1 < q < p$; but q would then divide n, so belong to Φ, and would be smaller than p, contradicting the choice of p. We conclude that p is prime. □

Theorem 9.2. *There are infinitely many primes in $\mathbb{Z}$.*

Proof. If there were only finitely many positive primes $p_1, \dots, p_t$, the number $m := 1 + p_1 \cdots p_t$ would not be divisible by any p_i, and this would contradict the previous lemma. □

Lemma 9.3. *Let $p \in \mathbb{Z}\backslash\{-1, 0, 1\}$. Then p is prime if and only if it has the following property:*

whenever $p|ab$, $p|a$ or $p|b$.

Proof. Since an integer p is prime if and only if $-p$ is prime we can assume that p is positive.

($\Rightarrow$) The gcd $d = (p, a)$ is a positive integer dividing p so is either 1 or p. If $d = p$, then $p|a$ and we are done, so suppose that $d = 1$. By a result in Math 402, there are integers u, v such that $1 = pu + av$. Hence $b = pbu + abv$; but p divides pbu and ab, hence abv, so p divides $pbu + abv = b$.

($\Leftarrow$) To see that p is prime, suppose that d divides p. Write $p = dc$. It suffices to show that either c or d is ± 1. Suppose to the contrary that neither is ± 1. Then the absolute values of c and d are both ≥ 2, and hence the absolute values of c and d are both $\leq p/2$.

However, since p divides the product dc, the hypothesis implies that p divides either c or d. But p can't divide any positive integer $\leq p/2$, so we obtain a contradiction.

We conclude that either c or d is ± 1, and hence p is prime. □

Theorem 9.4 (The Fundamental Theorem of Arithmetic)**.** *Let n be an integer ≥ 2. Then n is a product of primes in a unique way: if*

$$n = p_1 p_2 \dots p_r = q_1 q_2 \dots q_s$$

with all the p_is and q_js positive primes, and $p_1 \leq \dots \leq p_r$ and $q_1 \leq \dots \leq q_s$, then $r = s$ and $p_i = q_i$ for all i.

Proof. By Lemma 9.1, there is a smallest positive prime dividing n, say p_1. Write $n = p_1 n_1$. Since $p_1 \geq 2$, $n_1 \leq \frac{1}{2}n$. Applying Lemma 9.1 to n_1 now, we can write $n = p_1 p_2 n_2$ with p_2 a prime and $2 \leq p_1 \leq p_2$ and $n_2 \leq \frac{1}{2^2}n$. Continueing in this way, we get

$$n = p_1 p_2 \dots p_t n_t \qquad \text{and} \quad n_t \leq \frac{1}{2^t} n.$$

This process will stop once $2^t > n$. Thus n is a product of primes.

Now suppose that $n = p_1 p_2 \dots p_r = q_1 q_2 \dots q_s$ as in the statement of the theorem. Since p_1 is prime and divides $q_1 q_2 \dots q_s$, it must equal some q_i. But $q_1 \leq q_i = p_1$ and p_1 is the smallest positive prime dividing n, so $p_1 = q_1$. Hence

$$\frac{n}{p_1} = p_2 \dots p_r = q_2 \dots q_s$$

and repeating the argument we get $p_2 = q_2$, ... et cetera. □

More Exercises.

We will write $[r]$ to denote the image of an element $r \in R$ in a quotient ring R/I. That is, $[r] = r + I$, the coset of I containing r.

The 25 elements in the field $K = \mathbb{F}_5[x]/(f)$, where $f = x^2 + x + 1$, are

$$\{0, a^i \mid 1 \leq i \leq 24\} = \{\alpha a + \beta \mid \alpha, \beta \in \mathbb{F}_5\},$$

where $a = [3x + 1]$.

(1) Fill in the missing powers of a in the following table:

	$a^7 = 2a$	$a^{13} = 4a$	$a^{19} = 3a$
$a^2 = 4a + 3$	$a^8 = 3a + 1$	$a^{14} = a + 2$	$a^{20} = 2a + 4$
$a^3 =$	$a^9 =$	$a^{15} =$	$a^{21} =$
$a^4 = 3a + 2$	$a^{10} = a + 4$	$a^{16} = 2a + 3$	$a^{22} = 4a + 1$
$a^5 = 4a + 4$	$a^{11} = 3a + 3$	$a^{17} = a + 1$	$a^{23} = 2a + 2$
$a^6 = 2$	$a^{12} = 4$	$a^{18} = 3$	$a^{24} = 1$

(2) Write $[x]$ in the form $\alpha a + \beta$, with $\alpha, \beta \in \mathbb{F}_5$.
(3) Write $[x^3 + 2x + 4]$ in the form $\alpha a + \beta$, with $\alpha, \beta \in \mathbb{F}_5$.
(4) Find at least 2 zeroes in K of $g = t^8 + t^4 + 1 \in K[t]$. (Hint—factor $y^3 - 1$ and $z^{12} - 1$.)
(5) Why is the ring $F = \mathbb{F}_{19}[x]/(x^2 + 5)$ a field?
(6) Find the two square roots of 15 in the field F.
(7) Find the zeroes in F of the polynomial $f(y) = y^2 + 3y + 8 \in F[y]$ by using the quadratic formula

$$y = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

Friendly advice: plug your answer into $f(y)$ and check you get zero!

(8) Give an explicit isomorphism $\theta : F \to \mathbb{F}_{19}[t]/(t^2 + 1)$.

10. Divisibility and Factorization

The notion of division makes sense in any ring, and much of the initial impetus for the development of abstract algebra arose from problems of division and factorization, especially in rings closely related to the integers such as $\mathbb{Z}[\sqrt{d}]$. Division and factorization in polynomial rings is also of great importance.

Definition 10.1. Let a and b be elements of a commutative ring R. We say that a divides b in R if $b = ar$ for some $r \in R$.

We then call b a multiple of a and write $a|b$. ◊

Every element divides zero.

Zero divides no elements other than itself. At the other end of the spectrum, 1 divides every element. But 1 is not the only element with this property; a unit u divides every element because $b = u(u^{-1}b)$. Conversely, if u divides every element of R it is a unit.

10.1. **Greatest common divisors.** Let R be a domain. A greatest common divisor of two elements $a, b \in R$ is an element $d \in R$ such that

(1) $d|a$ and $d|b$, and
(2) if $e|a$ and $e|b$, then $e|d$.

We write $d = \gcd(a, b)$, or just $d = (a, b)$. We say that greatest common divisors exist in R if every pair of elements in R has a greatest common divisor in R.

The greatest common divisor is not unique. For example, in the ring of integers, both 2 and -2 are greatest common divisors of 6 and 10. Similarly, in $\mathbb{Z}[i]$ both 2 and $2i$ are greatest common divisors of 4 and 6.

Lemma 10.2. *Let R be a domain. If d and d' are greatest common divisors of a and b, then each is a unit multiple of the other.*

Proof. Because d and d' divide each other, we have $d' = du$ and $d = d'v$, for some elements u and v. Hence $duv = d$; because R is a domain and d is non-zero, we may cancel to get $uv = 1$. □

To obtain uniqueness of a greatest common divisor we need some additional structure on R. For example, in $\mathbb{Z}$ if we also insist that the greatest common divisor be positive, then it becomes unique.

Actually, we haven't even shown that greatest common divisors exist in $\mathbb{Z}$ or $\mathbb{Z}[\sqrt{d}]$. There is something to do here.

We can define the greatest common divisor of any collection of elements by saying that d is a greatest common divisor of $a_1, \ldots, a_n$ if it divides each a_i, and if e is any element of R dividing all of them, then e necessarily divides d.

Exercise. Sometimes we write (a, b) for the greatest common divisor of two integers a and b. This notation is also used to denote the ideal generated by a and b. For some rings there is an equality of ideals, $(a, b) = (d)$, when d is a greatest common divisor of a and b.

Show that 1 is a greatest common divisor of 2 and x in $\mathbb{Z}[x]$. What is the greatest common divisor of x and y in $\mathbb{C}[x, y]$?

10.2. **Primes and Irreducibles.**

Definition 10.3. Let R be a commutative ring. A non-zero non-unit $a \in R$ is
irreducible if in every factorization $a = bc$ either b or c is a unit;
prime if whenever $a|bc$ either $a|b$ or $a|c$. ◊

Lemma 10.4. *In a commutative domain every prime is irreducible.*

Proof. Let p be prime. If $p = bc$ then, perhaps after relabelling the factors, $p|b$, so $b = pu$ and $p = puc$; we can cancel in a domain, so $1 = uc$, whence c is a unit. □

The converse of this lemma is not always true: an irreducible need not be prime (see Example 10.8 below).

In order to give such an example we introduce some more general considerations.

10.3. **Quadratic extensions of the integers.** Let d be a non-square integer. The ring

$$\mathbb{Z}[\sqrt{d}] := \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\}$$

is called a quadratic extension of the integers.

Rings such of these have played, and continue to play, a central role in number theory.

Factorization and divisibility questions in $\mathbb{Z}[\sqrt{d}]$ are tackled by making use of what one knows about factorization and divisibility in $\mathbb{Z}$, and this is done by making use of the norm function: the norm of an element $x = a + b\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$ is

$$N(x) := a^2 - b^2 d.$$

If d is a negative integer the norm of an element x in $\mathbb{Z}[\sqrt{d}]$ is equal to $x\bar{x} = |x|^2$, where $\bar{x}$ is its complex conjugate.

The two fundamental properties of the norm are given in the next lemma, the proof of which is trivial (notice the proof of (1) uses the fact that d is not a square.

Lemma 10.5. *Let $x, y \in \mathbb{Z}[\sqrt{d}]$. Then*

(1) $N(x) = 0 \Leftrightarrow x = 0$.
(2) $N(xy) = N(x)N(y)$.

Because the norm is an integer, a factorization $a = xy$ in $\mathbb{Z}[\sqrt{d}]$ implies the the factorization $N(a) = N(x)N(y)$ in $\mathbb{Z}$. This provides a tool for studying factorization questions in $\mathbb{Z}[\sqrt{d}]$.

Lemma 10.6. *Let d be a negative integer.*

(1) *The element $x = a + b\sqrt{d}$ is a unit in $\mathbb{Z}[\sqrt{d}]$ if and only if $N(x) = 1$.*
(2) *The units in $\mathbb{Z}[i]$ are $\{\pm 1, \pm i\}$.*
(3) *If $d \neq -1$, the units in $\mathbb{Z}[\sqrt{d}]$ are $\{\pm 1\}$.*

Proof. Since $d < 0$, $N(x) \geq 0$. Certainly, if x is a unit, then $1 = N(1) = N(xx^{-1}) = N(x)N(x^{-1})$, so we conclude that $N(x) = 1$. Conversely, suppose that $N(x) = 1$. Then $x \neq 0$, and it has an inverse in $\mathbb{C}$, namely

$$x^{-1} = \frac{1}{a + b\sqrt{d}} . \frac{a - b\sqrt{d}}{a - b\sqrt{d}} = \frac{a - b\sqrt{d}}{a^2 - b^2 d} = a - b\sqrt{d}.$$

This belongs to $\mathbb{Z}[\sqrt{d}]$ so x is a unit in $\mathbb{Z}[\sqrt{d}]$.

The only way $a^2 - b^2 d$ can equal 1 is if $a^2 = 1$ and $b = 0$, leading to the units ± 1, or if $a = 0$, $d = -1$ and $b^2 = 1$, leading to the units $\pm i$ in $\mathbb{Z}[i]$. □

Example 10.7. Determining the units in $\mathbb{Z}[\sqrt{d}]$ is more complicated if d is a positive integer. For example, $1 + \sqrt{2}$ and $1 - \sqrt{2}$ are units in $\mathbb{Z}[\sqrt{2}]$, and $2 \pm \sqrt{5}$ are units in $\mathbb{Z}[\sqrt{5}]$. ◊

Example 10.8. An irreducible need not be prime. Let $R = \mathbb{Z}[\sqrt{-5}]$. We claim that 2 is irreducible in R but not prime.

It is easy to see that 2 is not prime because although it does not divide either $1 + \sqrt{-5}$ or $1 - \sqrt{-5}$ in $\mathbb{Z}[\sqrt{-5}]$, it divides their product:

$$(1 + \sqrt{-5})(1 - \sqrt{-5}) = 6 = 2.3.$$

To see that 2 is irreducible, suppose that $2 = bc$ where $b, c \in R$. Then

$$4 = N(2) = N(b)N(c).$$

If $b = x + y\sqrt{-5}$, then $N(b) = x^2 + 5y^2$, and the only way $N(b)$ could divide 4 is if $y = 0$ and $x = \pm 2$; so the only factorizations of 2 in $\mathbb{Z}[\sqrt{-5}]$ are $2 = 2.1 = (-2).(-1)$; since one of the factors is a unit, we see that 2 is irreducible. ◊

Exercise. Show that 2 is not prime in $\mathbb{Z}[i]$. Describe exactly which prime integers remain prime in $\mathbb{Z}[i]$.

10.4. **Unique factorization.**

Definition 10.9. A commutative domain R is a unique factorization domain, or UFD, if every element of R can be written uniquely as a product of irreducible elements, and the irreducibles that occur in the factorization are unique up to order and multiplication by units. ◊

To see what "uniqueness" means in this definition, consider the factorizations

$$6 = 2.3 = (-3).(-2) = (-3).(-1).(2).(-1).(-1)$$

in $\mathbb{Z}$. The uniqueness means this: if we have two factorizations of an element as a product of irreducibles, and x is an irreducible appearing in one of those factorizations, then some unit multiple of x must appear in the other factorization.

Lemma 10.10. *In a unique factorization domain, primes and irreducibles are the same.*

Proof. We observed on page 19 that a prime is irreducible.

Suppose that x is an irreducible and that $x|bc$. Then $bc = xy$ for some y. We can write each of b, c, and y, as a product of irreducibles. Doing so gives two factorizations of bc as a product of irreducibles. Buy the uniqueness of such a factorization, at least one of the irreducibles in the factorizations of b and c must be a unit mutiple of x. But that implies that x divides either b or c, thus showing that x is prime. □

Example 10.11. $\mathbb{Z}[\sqrt{-5}]$ is not a unique factorization domain because, as we showed in Example 10.8, the irreducible element 2 is not prime.

Indeed,

$$6 = 2.3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$$

gives two distinct factorizations of 6 as a product of irreducibles. We already showed that 2 is irreducible, and a similar argument shows that 3 is irreducible. To see that $1 + \sqrt{-5}$ is irreducible, write $1 + \sqrt{-5} = ab$ and suppose that a is not a unit. Then $6 = N(1 + \sqrt{-5}) = N(a)N(b)$. We already saw that there are no elements in $\mathbb{Z}[\sqrt{-5}]$ having norm 2 or 3, so it must be that $N(a) \in \{1, 6\}$. But a is not a unit, so $N(a) \neq 1$; it follows that $N(a) = 6$, and hence that $N(b) = 1$, so b is a unit.

Thus $1 + \sqrt{-5}$ is irreducible, and a similar argument shows that $1 - \sqrt{-5}$ is irreducible too. ◊

Historical remark. The notion of an *ideal* entered mathematics as a result of the failure of unique factorization to hold in certain rings. Originally, what we now call an ideal was called an "idealized number". The idea was to work with ideals rather than numbers: i.e., one could ask whether the ideal (6) in $\mathbb{Z}[\sqrt{-5}]$ can be written as *a product of prime ideals in a unique way.* Of course, one needs to define what one means by a prime ideal for this to make sense. But notice that an integer p is prime if and only if $\mathbb{Z}/(p)$ is a field; so we say that an ideal $\mathfrak{p}$ in $\mathbb{Z}[\sqrt{-5}]$ is prime if $\mathbb{Z}[\sqrt{-5}]/\mathfrak{p}$ is a field.

Notice that (2) is NOT a prime ideal in $\mathbb{Z}[\sqrt{-5}]$. To see this, observe that neither $a = 1 + \sqrt{-5}$ nor $b = 1 - \sqrt{-5}$ is in (2), i.e., neither a nor b is divisible by 2 in $\mathbb{Z}[\sqrt{-5}]$. Hence their images $\bar{a}$ and $\bar{b}$ in $\mathbb{Z}[\sqrt{-5}]/(2)$ are non-zero. However, $ab = 6$ *is* divisible by 2, so $ab \in (2)$ and this translates into the fact that in $\mathbb{Z}[\sqrt{-5}]/(2)$, $\bar{a}\bar{b} = 0$. Since $\mathbb{Z}[\sqrt{-5}]/(2)$ is not a domain it is not a field.

However, $(2, 1 + \sqrt{-5})$ *is* a prime ideal in $\mathbb{Z}[\sqrt{-5}]$, and so is $(2, 1 - \sqrt{-5})$. Similarly, the ideals $(3, 1 + \sqrt{-5})$ and $(3, 1 - \sqrt{-5})$ are prime, and we have the following factorization of (6) as a product of prime ideals:

$$(6) = (2, 1 + \sqrt{-5})^2.(3, 1 + \sqrt{-5}).(3, 1 - \sqrt{-5}).$$

In fact, every non-zero ideal in $\mathbb{Z}[\sqrt{-5}]$ can be written as a product of prime ideals in a unique way. This result (which actually extends to many other rings) is a very good replacement for the Fundamental Theorem of Arithmetic.

This is typical of how mathematics develops. One has a result (here the Fundamental Theorem of Arithmetic) that is enormously useful and one would like it to hold in new situations. Unfortunately it does not, so one modifies the original idea in some clever way (here by introducing ideals rather than numbers, and prime ideals rather than prime elements) so that a modified version of the original result is now true.

Mathematicians are tricky—we want something to be true so we introduce new concepts and ideas so that it is true (or at least an appropriate modified version is true).

A couple of people have asked about the official definition of a prime ideal. It is this: an ideal $\mathfrak{p}$ in a commutative ring R is prime if $R/\mathfrak{p}$ is a domain. Thus, in $\mathbb{Z}$, 0 is a prime ideal. In rings like $\mathbb{Z}[\sqrt{d}]$ it turns out that an ideal $\mathfrak{p}$ is prime if it is either zero or $\mathbb{Z}[\sqrt{d}]/\mathfrak{p}$ is a field.

Example 10.12. The ring $R = k[t, t^{1/2}, t^{1/4}, \cdots]$ is a domain in which prime and irreducible elements are the same but it is not a UFD. It fails to be a UFD because some elements, t for example, cannot be written as a product of irreducibles. To see that every irreducible is prime, suppose that x is irreducible and that $x|yz$. There is a suitably large n such that x, y, and z, all belong to $= k[t, t^{1/2}, \cdots, t^{1/2^n}]$; this subring is equal to $k[t^{1/2^n}]$ which is a polynomial ring in one variable (so a UFD); since x is still irreducible as an element of $k[t^{1/2^n}]$ it is prime in $k[t^{1/2^n}]$, so must divide either y or z; hence x is prime in R. $\Diamond$

Some Exercises.

In all these exercises, the elements $a, b, c \ldots$ belong to a commutative ring R. Similarly, I and J denote ideals in a commutative ring R. All rings are assumed to have an identity $1 \neq 0$.

(1) Show that IJ is an ideal if I and J are ideals.
(2) If J is an ideal in R containing an ideal I, show that J/I is an ideal of R/I. Show every ideal of R/I is obtained in this way.
(3) If J is an ideal in R containing an ideal I, show that
$$(R/I)/(J/I) \cong R/J.$$
Hint: use Proposition 7.12.
(4) Show that there is a 1-1 correspondence between the ideals in R/I and the ideals in R that contain I.

(5) Show that $\mathbb{Z}[\sqrt{-5}]/(1+\sqrt{-5}) \cong \mathbb{Z}_6$. The way to do this is to construct a surjective ring homomorphism $\phi : \mathbb{Z}[\sqrt{-5}] \to \mathbb{Z}_6$ such that $\ker \phi = (1+\sqrt{-5})$ and appeal to Proposition 7.12. In particular, you will need $\phi(1+\sqrt{-5}) = 0$. However, a ring homomorphism must, by definition, send the identity to the identity, so you now know what $\phi(\sqrt{-5})$ must equal. Now, you can figure out how to define ϕ on all elements of $\mathbb{Z}[\sqrt{-5}]$ because

$$\phi(x + y\sqrt{-5}) = \phi(x) + \phi(y)\phi(\sqrt{-5}).$$

So, with all these hints go ahead and prove that $\mathbb{Z}[\sqrt{-5}]/(1+\sqrt{-5}) \cong \mathbb{Z}_6$. Make sure that when you define ϕ you show that it really is a ring homomorphism—the tricky point will be to show that $\phi(ab) = \phi(a)\phi(b)$.

(6) Use the previous problem and the fact that

$$\frac{R}{I+J} \cong \frac{R/I}{(I+J)/I}$$

to show that $\mathbb{Z}[\sqrt{-5}]/(2, 1+\sqrt{-5}) \cong \mathbb{F}_2$, the field with two elements.

(7) Show that $\mathbb{Z}[\sqrt{-5}]/(3, 1+\sqrt{-5}) \cong \mathbb{F}_3$, the field with three elements.

(8) Decide whether the following integers remain prime in $\mathbb{Z}[i]$: $2, 3, 5, 7, 11, 13$. Do you detect a pattern? Can you conjecture a general result?

(9) Is there a ring homomorphism $\phi : \mathbb{Z}[\sqrt{-5}] \to \mathbb{F}_7$ such that $\phi(\sqrt{-5}) = 2$? Explain.

(10) Is there a ring homomorphism $\phi : \mathbb{Z}[\sqrt{-5}] \to \mathbb{F}_{11}$ such that $\phi(\sqrt{-5}) = 2$? Explain.

11. Arithmetic in $k[x]$

In $k[x]$, if we insist that the greatest common divisor of two polynomials be a monic polynomial, meaning that its leading coefficient is one, it becomes unique.

Proposition 11.1. *If f and g are non-zero elements of $k[x]$ such that f is non-zero, then there are unique polynomials q and r such that*

$$g = fq + r \qquad \text{and} \qquad \deg r < \deg f.$$

Proof. Existence. We argue by induction on $\deg g$. If $g = 0$, we can take $q = r = 0$. If $\deg g < \deg f$, we can take $q = 0$ and $r = g$. If $m = \deg g \geq \deg f = n$, we can write

$$g = \alpha x^m + \cdots \text{lower degree terms}$$
$$f = \beta x^n + \cdots \text{lower degree terms}.$$

Since

$$\deg\big(g - \alpha\beta^{-1}x^{m-n}f\big) < \deg g,$$

we may apply the induction hypothesis to $g - \alpha\beta^{-1}x^{m-n}f$.

Uniqueness. If $g = fq + r = fq' + r'$, then $f(q - q') = r' - r$. But $\deg(r' - r) < \deg f$, so this implies that $r' - r = 0$. Hence $q' = q$ also. □

Proposition 11.2. *Every pair of non-zero elements in $k[x]$ has a greatest common divisor.*

Proof. To prove this, we need to introduce the Euclidean algorithm. The Euclidean algorithm is a constructive method that produces the greatest common divisor of two polynomials, as we now show. □

The Euclidean algorithm. Let f and g be elements of $k[x]$ with f non-zero. By repeatedly using Proposition 11.1 we may write

$$\begin{aligned} g &= fq_1 + r_1 \qquad \text{with} \qquad \deg r_1 < \deg f, \\ f &= r_1q_2 + r_2 \qquad \text{with} \qquad \deg r_2 < \deg r_1, \\ r_1 &= r_2q_3 + r_3 \qquad \text{with} \qquad \deg r_3 < \deg r_2, \\ \cdots &\quad \cdots . \end{aligned}$$

Since the degrees of the remainders r_i are strictly decreasing, this process must stop. Stopping means that the remainder must eventually be zero. If $r_{t+2} = 0$, and we set $r_{-1} = g$ and $r_0 = f$, then the general equation becomes

$$r_i = r_{i+1}q_{i+2} + r_{i+2} \qquad \text{with} \qquad \deg r_{i+2} < \deg r_{i+1}, \tag{11-1}$$

and the last equation becomes

$$r_t = r_{t+1}q_{t+2}.$$

Claim: $r_{t+1} = \gcd(f, g)$. Proof: Since r_{t+1} divides r_t, it follows from (11-1) that r_{t+1} also divides r_{t-1}. By descending induction, (11-1) implies that r_{t+1} divides all r_i, $i \geq -1$. In particular, r_{t+1} divides f and g. On the other hand, if e divides both f and g, then it divides r_1. If e divides r_i and r_{i+1}, then it follows from (11-1) that it also divides r_{i+2}. By induction, e divides r_{t+1}. Hence r_{t+1} is a greatest common divisor of f and g. $\Diamond$

This proceedure for finding the greatest common divisor of f and g is called the Euclidean algorithm. It completes the proof of Proposition 11.2.

If K is a field containing k, then $K[x]$ contains $k[x]$. Hence, if f and g belong to $k[x]$, we can ask for their greatest common divisor in $k[x]$, and for their greatest common divisor in $K[x]$. These are the same. This is because the uniqueness of q and r in Proposition 11.1 ensures that carrying out the Euclidean algorithm in $k[x]$ for a pair $f, g \in k[x]$ produces exactly the same result as carrying out the Euclidean algorithm in $K[x]$ for that pair.

Proposition 11.3. *Let d be a greatest common divisor in $k[x]$ of non-zero elements f and g. Then $d = af + bg$ for some a and b.*

Proof. Since a greatest common divisor is unique up to a scalar multiple, we can assume that $d = r_{t+1}$, the last remainder produced by Euclidean algorithm. Working backwards, we have

$$r_{t+1} = r_{t-1} - r_tq_{t+1} = r_{t-1} - (r_{t-2} - r_{t-1}q_t)q_{t+1} = \cdots,$$

and so on. Eventually we obtain an expression in which every term is a multiple of either $r_0 = f$ or $r_{-1} = g$. Hence the result. $\square$

Let $f \in k[x]$. We write (f) for the set of all multiples of f. That is,

$$(f) = \{fg \mid g \in k[x]\}.$$

It is clear that (f) contains zero. The sum and difference of two multiples of f are multiples of f. Any multiple of a multiple of f is a multiple of f. Hence (f) is an ideal of $k[x]$. We call it the principal ideal generated by f.

Theorem 11.4. *Every ideal in $k[x]$ is principal.*

Proof. The zero ideal consists of all multiples of zero, so is principal. If I is a non-zero ideal, choose a non-zero element f in it of minimal degree. Clearly $(f) \subset I$. If g is an element of I, we may write $g = fq + r$ with $\deg r < \deg f$. However, r equals $g - fq$, so belongs to I; because the degree of f was minimal, we conclude that $r = 0$. Hence $g \in (f)$. Thus $I = (f)$. □

Notice that (f) is generated by λf if λ is a non-zero element of k. Conversely, if $(f) = (g)$, then g and f must be multiples of each other, so $g = \lambda f$ for some non-zero λ in k. Hence, if I is a non-zero ideal in $k[x]$, there is a *unique* monic polynomial f such that $I = (f)$.

Proposition 11.5. *The following conditions on a non-zero, non-unit $f \in k[x]$ are equivalent:*

(1) *f is irreducible;*
(2) *(f) is a maximal ideal;*
(3) *$k[x]/(f)$ is a field.*

Proof. By Lemma 7.17, conditions (2) and (3) are equivalent, so we only need prove the equivalence of (1) and (2).

(1) ⇒ (2) Suppose that f is irreducible, and that $(f) \subset (a) \neq k[x]$. Then $f = ab$ for some b, and a is not a unit because $1 \notin (a)$; because f is irreducible, b must be a unit. Thus $a = fb^{-1}$, so every multiple of a is a multiple of f, whence $(a) \subset (f)$, and we deduce that $(f) = (a)$ showing that (f) is maximal.

(2) ⇒ (1) Suppose that $f = ab$; we must show that either a or b is a unit. Suppose that a is not a unit. Then $(a) \neq k[x]$. But every multiple of f is a multiple of a, so $(f) \subset (a)$, and the hypothesis that (f) is maximal implies that $(f) = (a)$. In particular, $a = fu$ for some $u \in k[x]$, whence $f = ab = fub$ and $1 = ub$ because we can cancel in a domain. Thus b is a unit, showing that f is irreducible. □

The simplest illustration of Propositon 11.5 is provided by $k[x]/(x - \lambda)$ where $\lambda \in k$. Every polynomial of degree one is irreducible, so $k[x]/(x - \lambda)$ is a field. Which field? It is k because $(x - \lambda)$ is the kernel of the evaluation homomorphism $\varepsilon : k[x] \to k$, $\varepsilon(f) = f(\lambda)$.

Example 11.6. Let $f \in \mathbb{R}[x]$ be a monic polynomial of degree two. If f has a real zero, it is not irreducible in $\mathbb{R}[x]$. Suppose f has no real zero. Then it is irreducible in $\mathbb{R}[x]$, so $\mathbb{R}[x]/(f)$ is a field. Which field? It is $\mathbb{C}$ because, if $\alpha \in \mathbb{C}$ is a zero of f, (f) is the kernel of the evaluation homomorphism $\varepsilon : \mathbb{R}[x] \to \mathbb{C}$, $\varepsilon(f) = f(\alpha)$. (Why is ε surjective?)

It is perhaps good for your health to see explicitly which element(s) of $\mathbb{R}[x]/(f)$ square to -1. The way to do this is to complete the square: if $f = x^2 + 2bx + c$, then in $\mathbb{R}[x]/(f)$ we have

$$(x + b)^2 = b^2 - c;$$

because f has no real zero, $b^2 - c < 0$, whence $\sqrt{c - b^2} \in \mathbb{R}$; so the square of the image in $\mathbb{R}[x]/(f)$ of $\sqrt{c - b^2}(x + b)$ is -1. ◊

Proposition 11.5 provides a huge source of fields. For example, if $d \in \mathbb{Q}$ is not a square, then $\mathbb{Q}[x]/(x^2 - d)$ is isomorphic to $\mathbb{Q}(\sqrt{d})$.

Algebraic and transcendental elements. Let K be a field and k a subfield of K. An element $a \in K$ is said to be algebraic over k if it is a zero of a non-zero

polynomial with coefficients in k. That is, if

$$\lambda_n a^n + \lambda_{n-1} a^{n-1} + \cdots + \lambda_1 a + \lambda_0 = 0$$

for some $\lambda_0, \ldots, \lambda_n \in k$, not all zero. Equivalently, a is algebraic over k if and only if the homomorphism $\varepsilon : k[x] \to K$ given by $\varepsilon(f) = f(a)$ is not injective.

If a is not algebraic over k we say it is transcendental over k.

We say that k is algebraically closed if the only elements algebraic over k (whatever K may be) are the elements of k itself.

Proposition 11.7. *Let k be a field. The following are equivalent:*

(1) *k is algebraically closed;*
(2) *the only irreducible polynomials in $k[x]$ are the degree one polynomials;*
(3) *every polynomial in $k[x]$ of positive degree has a zero in k.*

Exercise. Factor $x^7 - 1$ as a product of irreducible polynomials in $\mathbb{F}_2[x]$, $\mathbb{F}_3[x]$, and $\mathbb{F}_7[x]$.

12. Zeroes of polynomials

One of the great motivating problems for the development of algebra was the question of finding the zeroes, or roots, of a polynomial in one variable.

The question of whether an element $\alpha \in k$ is a zero of a polynomial $f \in k[x]$ can be expressed formally as follows: *is f in the kernel of the ring homomorphism $\varepsilon_\alpha : k[x] \to k$ defined by*

$$\varepsilon_\alpha(f) = f(\alpha)?$$

You should check that ε_α is a ring homomorphism; indeed, the ring structure on $k[x]$ is defined just so this is a homomorphism. The kernel of ε_α is an ideal, and obviously contains $x - \alpha$ and therefore the ideal $(x - \alpha)$. However, $(x - \alpha)$ is a maximal ideal. We therefore have the following result.

Lemma 12.1. *If $f \in k[x]$, then $x - \alpha$ divides f if and only if $f(\alpha) = 0$.*

Definition 12.2. Let $\alpha \in k$ and $0 \neq f \in k[x]$. We say that α is a zero of f of multiplicity n if $(x - \alpha)^n$ divides f but $(x - \alpha)^{n+1}$ does not. ◊

Proposition 12.3. *Let f be a monic polynomial in $k[x]$. If $\alpha_1, \ldots, \alpha_r$ are the distinct zeroes of f, and α_i is a zero of multiplicity n_i, then*

$$f = (x - \alpha_1)^{n_1} \cdots (x - \alpha_r)^{n_r} g$$

where g is a polynomial having no zeroes in k.

Proof. We argue by induction on the number of zeroes and multiplicity, cancelling a factor of the form $x - \alpha$ at each step. □

The next result and its corollary are among my favorite results in mathematics—the proof is very devious. It shows that if f is a non-constant polynomial with coefficients in a field k, then there is a larger field K in which f has a zero. Of course, the first example that comes to mind is the polynomial $x^2 + 1$ in which case $\mathbb{C}$, the field of complex numbers, contains a zero of the polynomial. However, notice that the proof is essentially a tautology.

A field K is called an extension of a field k if k is a subfield of K.

Theorem 12.4. *Let $f \in k[x]$ be an irreducible polynomial. Then there is a field $K \supset k$ and an element $\alpha \in K$ such that $f(\alpha) = 0$.*

Proof. Since f is irreducible $K := k[x]/(f)$ is a field. Let $\alpha = \bar{x} = x + (f)$ be the image of x in K. If $f = \sum a_i x^i$, then, computing in K, we have

$$f(\alpha) = \sum a_i \alpha^i = \sum (a_i + (f))(x + (f))^i = \big(\sum a_i x^i + (f)\big) = (f + (f)) = 0$$

as claimed.

Alternatively, let $\pi : k[x] \to K$ denote the natural map, and write $\alpha = \pi(x)$. Then

$$f(\alpha) = \sum_{i=0}^{n} a_i \bar{x}^i = \pi\big(\sum_{i=0}^{n} a_i x^i\big) = \pi(f) = 0.$$

Hence α is a zero of f. □

Corollary 12.5. *Let $f \in k[x]$ be a monic polynomial. Then there is a field $K \supset k$ and elements $\alpha_i \in K$ such that $f = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n)$.*

Proof. We argue by induction on the degree of f. If $\deg f = 1$ there is nothing to prove. Write $f = gh$ where g is irreducible. Then $L := k[x]/(g)$ is a field and there is an $\alpha \in L$ such that $g = (x - \alpha)g'$ for some $g' \in L[x]$. Now consider f as an element in $L[x]$. As such it factors, say $f = (x - \alpha)f'$. By induction there is a field $K \supset L$ such that f' is a product of linear factors in $K[x]$. Hence f is a product of linear terms in $K[x]$. □

13. Principal ideal domains

Recall that every ideal in $\mathbb{Z}$ is of the form (d) for some d. Similarly, every ideal in $k[x]$ is of the form (f) (Theorem 11.4).

An ideal of the form (r) in a ring R is said to be principal.

Definition 13.1. A principal ideal domain is a domain in which every ideal is principal, i.e., every ideal consists of multiples of a single element. ◊

Using the Euclidean algorithm is the standard method to show that a ring is a principal ideal domain. The argument in Theorem 11.4 is typical.

Proposition 13.2. *Let R be a principal ideal domain. Then*

1. *greatest common divisors exist in R;*
2. *if $d = \gcd(a, b)$, then $d = ax + by$ for some $x, y \in R$;*
3. *every irreducible in R is prime.*

Proof. (1) and (2). The ideal $aR + bR$ is principal, so is equal to dR for some $d \in R$. Clearly, $d = ax + by$ for some $x, y \in R$, so it remains to show that d is a greatest common divisor of a and b. First, since a and b belong to dR, they are both divisible by d. Second, if e divides both a and b, then $aR + bR$ is contained in eR, so d is a multiple of e. Hence d is a greatest common divisor of a and b.

(3) Let a be irreducible, and suppose that $a|bc$. To show that a is prime, we must show it divides either b or c. Let $d = ax + by = \gcd(a, b)$. Since d divides a, either d is a unit or $a = du$ with u a unit. But $d|b$, so the second alternative implies that $a|b$. Now suppose that d is a unit; since a divides bc it also divides $acxd^{-1} + bcyd^{-1} = c(ax + by)d^{-1} = c$. Hence a is prime. □

Theorem 13.3. *Every principal ideal domain is a unique factorization domain.*

Proof. Let R be a PID and a a non-zero non-unit in R. We must show that a is a product of irreducibles in a unique way.

Uniqueness. Suppose that $a = a_1 \cdots a_m = b_1 \cdots b_n$ and that each a_i and b_j is irreducible. Without loss of generality we can assume that $m \leq n$. If $m = 1$, then we would be done. By Proposition 13.2, a_1 divides some b_j; relabel the b_js so that $a_1 | b_1$. Since a_1 and b_1 are irreducible, $b_1 = a_1 u$ for some unit u. Thus $a_2 \cdots a_m = (ub_2) \cdots b_n$. If $m = 1$, we would have $1 = (ub_2) \cdots b_n$ so n would have to be one also, and we would be finished. However, if $m > 1$ and by an induction argument we can reduce to the case $m = 1$.

Existence. Suppose to the contrary that a is not a product of irreducibles. Then a is not irreducible, so $a = a_1 b_1$ with a_1 and b_1 non-units. Since a is not a product of irreducibles, at least one of a_1 and b_1 is not a product of irreducibles. Relabelling if necessary, we can assume that a_1 is not a product of irreducibles. Thus a_1 is not irreducible, and we may write $a_1 = a_2 b_2$ with a_2 and b_2 non-units.

Continuing in this way, we obtain a sequence $a_1, a_2, \ldots$ of irreducible elements, and factorizations $a_i = a_{i+1} b_{i+1}$ into a product of non-units. This yields a chain

$$Ra \subset Ra_1 \subset Ra_2 \subset \cdots$$

of ideals. The union of an ascending chain of ideals is an ideal of R, and it is a principal ideal, say Rz, by hypothesis. Now z must belong to some Ra_i, but then $Rz \subset Ra_i \subset Ra_{i+1} \subset Rz$, so these ideals are equal. In particular, $a_{i+1} \in Ra_i$, so $a_{i+1} = a_i u$. It follows that $a_i = a_{i+1} b_{i+1} = a_i u b_{i+1}$, whence b_{i+1} is a unit. This is a contradiction.

We conclude that a must be a product of irreducibles. □

Proposition 13.4. *Let f be an element in a principal ideal domain R. The following are equivalent:*

(1) *f is irreducible;*
(2) *(f) is a maximal ideal;*
(3) *$R/(f)$ is a field;*
(4) *f is a prime.*

Proof. Lemma 7.17 shows that conditions (2) and (3) are equivalent. Theorem 13.3 and Lemma 10.10 shows that conditions (2) and (4) are equivalent.

(1) ⇒ (2). Suppose J is an ideal of R that contains (f). By hypothesis, J is principal, say $J = (g)$. Thus $f = gh$ for some $h \in R$. Since f is irreducible either g is a unit, in which case $J = R$, or h is a unit, in which case $g = fh^{-1}$ and $(g) = (f)$.

(2) ⇒ (1). Suppose that $f = gh$. Then $(f) \subset (g)$ so either $(g) = R$, in which case g is a unit, or $(g) = (f)$, in which case $g = fv$ for some $v \in R$ and $hv = 1$ so h is a unit. Thus f is irreducible. □

14. Vector spaces

Definition 14.1. Fix a field k. An abelian group $(V, +)$ is called a k-vector space if there is an action of k on V,

$$k \times V \to V, \quad (\alpha, v) \mapsto \alpha.v, \text{ or } \alpha v,$$

such that for all $u, v \in V$ and $\alpha, \beta \in k$,

(1) $\alpha(u + v) = \alpha u + \alpha v$,
(2) $(\alpha + \beta)v = \alpha v + \beta v$,

(3) $\alpha(\beta v) = (\alpha\beta)v$,
(4) $1.v = v$,
(5) $\alpha 0 = 0$.

$\Diamond$

Vector spaces are all around us and you have encountered many.

Let $n \geq 1$. The n-dimensional vector space $k^n = k \times \cdots \times k$ is the Cartesian product of n copies of k with action given by

$$\alpha.(\lambda_1, \ldots, \lambda_n) := (\alpha\lambda_1, \ldots, \alpha\lambda_n).$$

We also define $k^0 = \{0\}$ to be the k-vector space consisting of one element. We call it the zero vector space.

The polynomial ring $k[x]$ is a k-vector space with the action defined by

$$\alpha.(\lambda_0 + \lambda_1 x + \cdots + \lambda_n x^n) := \alpha\lambda_0 + \alpha\lambda_1 x + \cdots + \alpha\lambda_n x^n.$$

The principle that ensures $k[x]$ is a k-vector space applies to other situations: if R is any ring that contains k as a subring in such a way that $\alpha r = r\alpha$ for all $\alpha \in k$ and all $r \in R$, then R becomes a k-vector space via

$$\alpha.r = \alpha r.$$

The vector space axioms follow from the fact that R is a ring.

For example, the quotient rings $k[x]/I$ are k-vector spaces.

Definition 14.2. A subspace U of a k-vector space V is a subgroup of $(V, +)$ such that $\lambda u \in U$ whenever $\lambda \in k$ and $u \in U$. $\Diamond$

If R is a ring containing a field k, then every ideal I of R is a subspace of R. Similarly, if $I \subset J$ are ideals of R, then J/I is a subspace of R/I (because it is an ideal).

Definition 14.3. Let U and V be k-vector spaces. A k-linear map $f : U \to V$ is a group homomorphism such that $f(\lambda u) = \lambda f(u)$ for all $\lambda \in k$ and all $u \in U$. If f is, in addition, bijective we call it an isomorphism of vector spaces and write $U \cong V$. The inverse of an isomorphism is an isomorphism. $\Diamond$

Theorem 14.4. *Let $f : U \to V$ be a linear map between two k-vector spaces. Then* $\ker f := \{u \in U \mid f(u) = 0\}$ *is a subspace of U,* $\operatorname{im} f$ *is a subspace of V, and* $U/\ker f \cong \operatorname{im} f$.

If two rings R and S contain copies of the field k and $f : R \to S$ is a ring homomorphism such that $f(\lambda) = \lambda$ for all $\lambda \in k$, then f is a linear map.

Example 14.5. Let $V = k^n$, $n \geq 1$, and define $t : V \to k$ to be the linear map

$$t(\alpha_1, \ldots, \alpha_n) := \alpha_1 + \cdots + \alpha_n = \sum_{i=1}^{n} \alpha_i.$$

It is an easy matter to check that t is a linear map—you should do it.

One can jazz this up. If $\omega_1, \ldots, \omega_n$ are any elements of k, the map $w : V \to k$ defined by

$$w(\alpha_1, \ldots, \alpha_n) := \sum_{i=1}^{n} \omega_i \alpha_i$$

is linear (again, check). We call $w(\alpha_1, \dots, \alpha_n)$ a weighted sum. The map t in the previous paragraph is a special case of w.

The map w can be described in terms of matrix multiplication and this is useful because there are many excellent computer programs for efficient multiplication of matrices. In this case we have

$$w(\alpha_1, \dots, \alpha_n) = (\alpha_1, \dots, \alpha_n) \begin{pmatrix} \omega_1 \\ \vdots \\ \omega_n \end{pmatrix} = (\omega_1, \dots, \omega_n) \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix}$$

$\Diamond$

Example 14.6. The map $w : \mathbb{F}_{11}^{10} \to \mathbb{F}_{11}$ defined by

$$w(\alpha_1, \dots, \alpha_{10}) := \sum_{i=1}^{10} i\alpha_i$$

is a linear map. You should check this. The kernel of w consists of what are called ISBNs, International Standard Book Numbers. If you pick a book off your book shelf you will find, perhaps on the back, perhaps on one of the early pages, a 10-digit number, for example, 3-540-60168-6, that uniquely identifies the book. The first digit identifies the language, the next three the publisher, the next five the book on that publishers list, and the last is a check digit. What we mean by that is that the first 9 digits, $\alpha_1, \dots, \alpha_9$ are determined by the book, but α_{10} is chosen exactly so that $(\alpha_1, \dots, \alpha_{10})$ belongs to $\ker(w)$. This can be done because once $\alpha_1, \dots, \alpha_9$ are known and viewed as elements of $\mathbb{F}_{11}$, one knows $a_1 + 2\alpha_2 + \cdots + 9\alpha_9 \in \mathbb{F}_{11}$ and if one now sets $\alpha_{10} := a_1 + 2\alpha_2 + \cdots + 9\alpha_9$, then $a_1 + 2\alpha_2 + \cdots + 9\alpha_9 + 10\alpha_{10} = 0$ so $(\alpha_1, \dots, \alpha_{10})$ belongs to $\ker(w)$. When you enter an ISBN into a computer system it checks that it belongs to $\ker(w)$; if you mistype one of the digits the computer will know that you made an error because what you have entered will not belong to $\ker(w)$.

It is possible that $\alpha_{10} = 10$ but the letter X is used to denote that element of $\mathbb{F}_{11}$; for example, 0-521-22909-X is a valid ISBN number. $\Diamond$

Example 14.7. Let

$$A = \begin{pmatrix} \alpha_{11} & \dots & \alpha_{1m} \\ \vdots & & \vdots \\ \alpha_{n1} & \dots & \alpha_{nm} \end{pmatrix}$$

be an $n \times m$ matrix with entries in the field k. View the elements of k^m as column vectors

$$u = \begin{pmatrix} \beta_1 \\ \vdots \\ \beta_m \end{pmatrix}.$$

Define a linear map $f : k^m \to k^n$ by

$$f(u) = Au$$

for each $u \in k^m$ where A is the matrix above. Explicitly,

$$f(\beta_1, \dots, \beta_m) = \begin{pmatrix} \alpha_{11} & \dots & \alpha_{1m} \\ \vdots & & \vdots \\ \alpha_{n1} & \dots & \alpha_{nm} \end{pmatrix} \begin{pmatrix} \beta_1 \\ \vdots \\ \beta_m \end{pmatrix}.$$

The fact that f is a linear map follows easily from the basic properties of matrix multiplication and addition. Indeed, matrices were introduced, and their product and sum were defined, just so that every linear map $f : k^m \to k^n$ is of the form $u \mapsto Au$ for a suitable $n \times m$ matrix A.

We can also describe each linear map $f : k^m \to k^n$ as *right* multiplication by an $m \times n$ matrix as oppposed to left multiplication by an $n \times m$ matrix. For example, the map in the previous paragraph is also given by

$$f(\beta_1, \dots, \beta_m) = \begin{pmatrix} \beta_1 & \cdots & \beta_m \end{pmatrix} \begin{pmatrix} \alpha_{11} & \dots & \alpha_{n1} \\ \vdots & & \vdots \\ \alpha_{1m} & \dots & \alpha_{nm} \end{pmatrix}$$

$\Diamond$

15. Bases and dimension

Perhaps the most important notion needed for the analysis of a vector space is that of a basis, which then leads to the notion of dimension.

Definition 15.1. A basis for a k-vector space V is a set $\mathcal{B} = \{v_i \mid i \in I\} \subset V$ such that every $v \in V$ can be expressed in a unique way as

$$v = \sum_{i \in I} \alpha_i v_i$$

for some $\alpha_i \in k$. We do allow the possibility that the index set I is infinite. $\Diamond$

Of course, for a given v at most a finite number of the coefficients α_i in the expression for v are non-zero (there is no way of making sense of an infinite sum in V).

The uniqueness part of the definition is vital. The span of a subset $\mathcal{B}$ of V is the set of $v \in V$ that can be expressed as a finite sum

$$v = \sum \alpha_i v_i \tag{15-1}$$

for some v_is in $\mathcal{B}$ and α_is in k. It is an easy exercise to show that the span of $\mathcal{B}$ is a subspace of V. We call an expression of the form (15-1) a linear combination of the v_is. $\mathcal{B}$ is a basis for the subspace it spans if and only if every element in that span can be expressed as a linear combination of elements in $\mathcal{B}$ *in a unique way*; this is equivalent to the condition that if $\sum \alpha_i v_i = 0$ with each $v_i \in \mathcal{B}$, then all α_i are zero.

Definition 15.2. The dimension of a vector space V is the cardinality of (number of elements in) a basis for V. $\Diamond$

The following result, which we will not prove, ensures that this makes sense.

Proposition 15.3. *Any two bases for a vector space have the same cardinality.*

We usually write $\dim V$ for the dimension of V, or $\dim_k V$ if we want to emphasize the field k.

The dimension of k^n is n. The vectors

$$e_1 = (1, 0, 0, \dots, 0),\ e_2 = (0, 1, 0, \dots, 0),\ \dots,\ e_n = (0, 0, \dots, 0, 1, 0),$$

form a basis for k^n because

$$(\lambda_1, \dots, \lambda_n) = \lambda_1 e_1 + \lambda_2 e_2 + \cdots + \lambda_n e_n,$$

and there is obviously no other way of writing $(\lambda_1, \dots, \lambda_n)$ as a linear combination of $e_1, \dots, e_n$ with coefficients in k.

Theorem 15.4. *Two k-vector spaces are isomorphic if and only if they have the same dimension.*

Proof. If U and V have bases $\mathcal{B}$ and $\mathcal{C}$ respectively having the same cardinality there is a bijection $t : \mathcal{B} \to \mathcal{C}$. We then define $f : U \to V$ by

$$f\left(\sum \alpha_i u_i\right) := \sum \alpha_i t(u_i)$$

for any α_is in k and u_is in $\mathcal{B}$. It is easy to check that f is a linera map, and that it has an inverse given by

$$f^{-1}(\sum \beta_j v_j) = \sum \beta_j t^{-1}(v_j)$$

where the v_js belong to $\mathcal{C}$ and the β_js to k.

Conversely, if $f : U \to V$ is an isomorphism and $\mathcal{B}$ is a basis for U it is easy to check that $\{f(u) \mid u \in \mathcal{B}\}$ is a basis for V. □

Corollary 15.5. *Up to isomorphism, the only vector spaces of finite dimension are the k^n, $n \geq 0$.*

Proposition 15.6. *If f is a polynomial of degree $n \geq 0$, then $\dim_k k[x]/(f) = n$, and the images of $1, x, \dots, x^{n-1}$ are a basis for $k[x]/(f)$.*

Proof. The natural homomorphism $\pi : k[x] \to k[x]/(f)$ sends k, the subring of constant polynomials, to an isomorphic copy of itself in $k[x]/(f)$, so we think of k as a subring of $k[x]/(f)$. Multiplication in $k[x]/(f)$ therefore gives $k[x]/(f)$ the structure of a k-vector space. Since the powers of x are a basis for $k[x]$, their images span $k[x]/(f)$.

If g is any element of $k[x]$, then $g = af + r$ for some $a \in k[x]$ and some r of degree $< n$. Since $\pi(g) = \pi(r)$ and since r is a linear combination of $1, x, \dots, x^{n-1}$, $\{\pi(x^i) \mid 0 \leq i \leq n-1\}$ spans $k[x]/(f)$. These elements are linearly independent too because the only linear combination of $1, x, \dots, x^{n-1}$ that belongs to (f) is $0.1 + 0.x + \cdots + 0.x^{n-1}$. □

Theorem 15.7. *If W is a subspace of a vector space U, then*

$$\dim \frac{U}{W} = \dim U - \dim W.$$

Amongst other things this says that the dimension of a subspace or quotient of U is no larger than that of U itself.

One trivial consequence of this result (that we use often) is that when W is a subspace of a finite-dimensional vector space U, $W = U$ if and only if $\dim W = \dim U$.

Consider the following special, but important, case of the theorem. Let f and g be non-zero polynomials in $k[x]$ such that g divides f. Then $(f) \subset (g)$ and we have the ring isomorphism

$$\frac{k[x]/(f)}{(g)/(f)} \cong \frac{k[x]}{(g)}.$$

This is also an isomorphism of k-vector spaces so

$$\deg(g) = \dim \frac{k[x]}{(g)} = \dim \frac{k[x]}{(f)} - \dim \frac{(g)}{(f)}$$

from which we see that

$$\dim \frac{(g)}{(f)} = \deg(f) - \deg(g).$$

If we set $n = \deg(f)$ and $d = \deg(g)$, then $(g)/(f)$ is a d-dimensional subspace of the n-dimensional vector space $k[x]/(f)$. This provides an important example of an (n, d)-linear code (see below).

Theorem 15.8. *Let $f : U \to V$ be a linear map between two vector spaces. Then*

(1) $\ker f$ *is a subspace of* U *and* $\operatorname{im} f$ *is a subspace of* V*,*
(2) $\operatorname{im} f \cong U/\ker f$*,*
(3) $\dim(\ker f) + \dim(\operatorname{im} f) = \dim U$*.*

Some Homework Problems

In all the exercises below we write $\mathbb{F}$ for the field with two elements.

(1) The first digit of an ISBN identifies the language in which it is published: for example, 0 for English, 2 for French, 3 for German. The next three digits identify the publisher. Suppose that the ISBN of a book published in German is 3-540. The English translation of it has an ISBN beginning 0-abc, and the rest of the ISBN is the *same* as for the German edition. Find *abc* in order for this to be true. Is there a unique such *abc*? Explain.
(2) If in entering an ISBN into the computer one transposes two adjacent digits can the computer detect the error?
(3) UPS identifies packages by assigning a 10 digit number consisting of nine digits plus a check digit: the check digit is the remainder modulo 7 of the 9-digit number. What percentage of single digit errors will this method recognize?
(4) Show that a finite domain is a field.
(5) Let K be a finite field. Why is the image of the natural ring homomorphism $\mathbb{Z} \to K$ isomorphic to $\mathbb{Z}_p$ for some prime p? We call this p the characteristic of K.
(6) If k is a subfield of a field K, then K can be viewed as a k-vector space in a natural way. Suppose that K is a finite field of characteristic p. Why must the number of elements in K be of the form p^n for some integer n?
(7) Let $K \subset L$ be finite fields. By the previous exercise there is a prime p and integers m and n such that $|K| = p^m$ and $|L| = p^n$. What is the relation between m and n (Hint: count the number of elements in k^n when k is a finite field).
(8) Let $\mathcal{B}$ be a subset of a vector space V. Show that $\mathcal{B}$ is not a basis if it contains distinct elements u, v, w, y, z such that $u + v = w + y + z$.
(9) Find a subset $\mathcal{B}$ of the following elements of $\mathbb{F}^6$ that provide a basis for $\mathbb{F}^6$:

000000, 011000, 001111, 111010, 010111, 110101, 100010, 101101, 101010, 111111, 010101.

Make sure you prove that the elements in $\mathcal{B}$ both span $\mathbb{F}^6$ and that they are linearly independent—you may prove the latter by showing that 0 can

be written in only one way as a linear combination of the elements in $\mathcal{B}$, namely the combination with all coefficients equal to zero.

16. Finite fields

Let K be a finite field. The group $(K, +)$ is finite, so $n.1 = 1 + \cdots + 1 = 0$ for some positive integer n. Let p be the smallest such integer. Then the natural ring homomorphism $\mathbb{Z} \to K$, $1 \mapsto 1$, has kernel (p). Hence K contains a copy of $\mathbb{F}_p$.

We call p the characteristic of K.

Proposition 16.1. *Let K be a finite field of characteristic p. Then $|K| = p^n$ for some n.*

Proof. We can view K as a vector space over its subfield $\mathbb{F}_p$. Because K is finite it has finite dimension, say n. Hence $K \cong \mathbb{F}_p^n$ as an $\mathbb{F}_p$-vector space. But $|\mathbb{F}_p^n| = p^n$. □

Lemma 16.2. *Let p be a prime, n a positive integer, and set $q = p^n$. Suppose a and b belong to a ring R in which $p = 0$. Then*

$$(a + b)^q = a^q + b^q.$$

Proof. We argue by induction on n. For $n = 1$ we have

$$(a + b)^p = \sum_{i=0}^{p} \binom{p}{i} a^i b^{p-i}.$$

If $1 \le i \le p - 1$, the binomial coefficient $\binom{p}{i}$ is divisible by p so is zero in R. Hence only the $i = 0$ and $i = p$ terms from the binomial expansion survive in R and give the result $(a + b)^p = a^p + b^p$.

Now suppose $n > 1$ and write $q = pr$. Then

$$(a + b)^q = \big((a + b)^r\big)^p = \big(a^r + b^r\big)^p = (a^r)^p + (b^r)^p = a^q + b^q,$$

as required. □

Theorem 16.3. *Let p be a prime and n a positive integer. Then*

1. *There is a field with p^n elements.*
2. *If K is a field with p^n elements then every element in K is a zero of the polynomial $x^{p^n} - x$.*

Proof. (2) Since $K^\times := K - \{0\}$ is a group with $p^n - 1$ elements, $a^{p^n - 1} = 1$ for all $a \in K - \{0\}$. Hence $a^{p^n} = a$ for all $a \in K$.

(1) Write $q = p^n$. Consider the polynomial $x^q - x \in \mathbb{F}_p[x]$. By Corollary 12.5, there is a field L containing $\mathbb{F}_p$ and elements $\alpha_1, \ldots, \alpha_q \in L$ such that

$$x^q - x = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_q).$$

Let K be the subset of L consisting of all the α_is. By the previous lemma, $\alpha_i + \alpha_j$ is again in K; so too is $\alpha_i \alpha_j$. Obviously, 0 and 1 are in K, and so too is α_i^{-1} if $\alpha_i \neq 0$. Hence K is a subfield of L.

It remains to show that K has exactly q elements, i.e., that $x^q - x$ is not divisible by $(x - \lambda)^2$ for any $\lambda \in L$. If it were, then λ would be a zero of both $x^q - x$ and its derivative, $qx^{q-1} - 1$. But that derivative is -1 because $p|q$ and $p = 0$ in $\mathbb{F}_p$ and hence in L. Hence $x^q - x$ is not divisible by $(x - \lambda)^2$, and we deduce that $|K| = q$. □

Theorem 16.4. *If K is a finite field, then $K^\times$ is a cyclic group.*

Proof. Let $e = |K^\times| = p_1^{n_1} \cdots p_t^{n_t}$ as a product of powers of distinct primes. Define

$$e_i := \frac{e}{q_i} \qquad \text{and} \qquad d_i := \frac{e}{q_i^{n_i}}.$$

Since the polyomial $x^{e_i} - 1$ has at most e_i zeroes, there is an $a_i \in K$ such that $a_i^{e_i} \neq 1$. Define $b_i := a_i^{d_i}$. Then $1 = a_i^e = b_i^{p_i^{n_i}}$, but

$$1 \neq a^{e_i} = b_i^{p_i^{n_i - 1}}$$

so b_i has order exactly $q_i^{n_i}$.

Claim: If G is an abelian group and $x, y \in G$ have relatively prime orders r and s, then xy has order rs. Proof: Let d denote the order of xy. Then $1 = (xy)^{ds} = x^{ds}$ so $r|ds$ and hence $r|d$. Similarly, $s|d$. Hence $rs|d$. But $(xy)^{rs} = 1$, so $d = rs$. $\Diamond$

An induction argument based on the claim now shows that the order of $b_1 b_2 \cdots b_t$ is e. Hence $K^\times$ is cyclic. $\square$

Proposition 16.5. *Let R be a commutative domain containing a field k. If $\dim_k R < \infty$, then R is a field.*

Proof. Fix $0 \neq a \in R$ and define $\phi : R \to R$ by $\phi(x) = ax$. Then ϕ is a k-linear map and is injective because R is a domain. Thus $\dim(\in \phi) = \dim R$ by Theorem 15.8. Hence $\operatorname{im} \phi = R$, so $1 = \phi(x)$ for some $x \in R$. Since $ax = 1$, a is a unit. $\square$

17. Linear Codes

Do not confuse coding theory with cryptography. In cryptography the key point is secrecy; one wishes to send a message in such a way that an unauthorized reader can not understand it. In coding theory secrecy is not an issue. Instead, the goal is to send a message in such a way that if a modest number of errors occur in transmission the recipient will still be able to recover the original message.

The process involved is the following. The sender begins with the original message, perhaps a photograph. According to some rules the message is translated into a string of zeroes and ones. Rather than thinking of this as a single long string of zeroes and ones we think of it as a long sequence of chunks, each chunk consisting of some specified number of bits. For example, if one has a photograph consisting of $1024 \times 1024 = 2^{20}$ pixels and each pixel can have one of $128 = 2^7$ color/brightness levels, then the message consists of 2^{20} chunks where each chunk consists of 7 bits. We call these chunks message words.

We do *not* send the message words. Instead we add some extra data to each message word in a clever way to create a code word and transmit the code word. Let's begin with two simple examples.

Example 17.1. The $(3,1)$-repetition code. Suppose a message word is a single bit, 0 or 1, and each message word is turned into a 3-bit code word by repeating it 3 times. Thus 000 is sent rather than 0 and 111 is sent instead of 1. If a single bit of a code word is changed in transmission one can recover the sent code word by taking the most frequently occurring digit; e.g., if one receives 101 it makes some sense to guess that 111 was sent. This allows us to correct one error and is therefore called a 1-error correcting code. However, if two errors are made in transmission we would not correctly decode the received word. $\Diamond$

Example 17.2. The $(4,1)$-repetition code. This code corrects one error and detects two errors. As in the previous example, a message word is a single bit, 0 or 1. Now each message word is turned into a 4-bit code word by repeating it 4 times. Thus 0000 is sent rather than 0 and 1111 is sent instead of 1. If a single bit of a code word is changed in transmission one can recover the sent code word by taking the most frequently occurring digit. The $(4,1)$-repetition code is better than the $(3,1)$-repition code in that if two errors are made in transmission we will recognize that because one cannot change a codeword to different codeword by making ≤ 2 errors. But this code will not correct two errors because if we receive 0011 there is no basis for reasonably arguing that one of 0000 and 1111 was sent rather than the other. $\Diamond$

In the photograph example, we might add another 8 bits to the 7 bits in each message word in a very particular way. This new chunk consisting of 15 bits is called a code word and it is the code word what we transmit. In coding theory such a 15-bit code word is viewed as an element of the 15-dimensional vector space $\mathbb{F}_2^{15}$. We often write C for the set of code words. In this example, C is a subset of $\mathbb{F}_2^{15}$ and consists of 2^8 elements, one code word for each possible message word.

The sequence of code words (i.e., the 2^{20} 15-bit code words in the photograph example) is called the encoded message and the process of translating the original message to the encoded one is called encoding.

The encoded message is now sent. There is a possibility, in some situations a virtual certainty, that errors will arise during transmission. A typical cause of such errors is electro-magnetic interference. In the photograph example, we send a code word $v \in C$ and the received word w is an element $\mathbb{F}_2^{15}$ *which generally will not be* v*, the word sent.* If a received word is a valid code word (i.e., $w \in C$) the receiver assumes that w was the code word sent. However, if the received word is not a valid code word (i.e., $w \notin C$) the recipient tries to correct w by replacing it by the code word that is "nearest to it". After the correction is made, one translates the code word back to the message word that corresponds to it. This process is called decoding.

The encoding and decoding process are of no interest to us here. If you absolutely must think about them, suppose for simplicity that the original message is in English, and one simply replaces the letter "a" by 000001, the letter "b" by 000010, etc. But, to repeat, we have no interest in this process, and will consider it no further.

Example 17.3. The $(3,2)$ parity check code. Suppose the original message is composed of the four message words

$$00,\ 01,\ 10,\ 11.$$

The message words are the four elements of the vector space $\mathbb{F}_2^2$. A message word is converted to a codeword by adding to the end of it

- a 0 if the message word has an even number of 1's;
- a 1 if the message word has an odd number of 1's.

The following table lists the message words and the corresponding code words:

Message Word	$\longrightarrow$	Code Word
00		000
01		001
10		101
11		110

The code words form a subset $C \subset \mathbb{F}_2^3$. A $v \in \mathbb{F}_2^3$ is a code word if and only if the sum of its digits is zero. The code words form a vector subspace of $\mathbb{F}_2^3$. They are the elements in the kernel of the linear map

$$\mathbb{F}_2^3 \to \mathbb{F}_2, \qquad (\alpha_1, \alpha_2, \alpha_3) \mapsto \alpha_1 + \alpha_2 + \alpha_3$$

(see Example 14.5). If we receive a word for which the sum of its digits is 1, we know an error must have occurred in the transmission. Thus, this code allows us to recognize if a single error occurred in the transmission of a word. But we are unable to make a good decision as to what the sent word was; for example, if we receive the word 001, the word sent might be 000, or 011, or 101, or something else—the three possibilities listed are those in which only a single bit is messed up during transmission. This is *not* an error correcting code.

Do not confuse C and $\mathbb{F}_2^2$. The message words belong to $\mathbb{F}_2^2$ and the code words belong to C; adding the appropriate digit to the end of a message word to produce a code word is an isomorphism $\mathbb{F}_2 \to C$. In fact, C is the image of the linear map $f : \mathbb{F}_2^2 \to \mathbb{F}_2^3$ given by

$$f(u) = uA$$

where

$$A = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}.$$

Thus the encoding procedure consists of right multiplication by A. ◊

Definition 17.4. Fix positive integers $k < n$. An (n, k) binary linear code is a k-dimensional subspace C of $\mathbb{F}_2^n$. We call C an (n, k)-code, or block code, or simply a code. Elements of C are called code words. ◊

Only code words are transmitted but due to errors in transmission *any* element of $\mathbb{F}_2^n$ might be received.

Each code word is simply a string of n 0s and 1s, and what is received is a string of zeros and ones. We make the assumption that all errors are equally likely: i.e., if we send a string of n zeroes and ones the probability that the i^{th} digit is changed is independent of i and independent of whether that digit is a zero or one. We also assume that multiple errors are independent.

Example 17.5. The rectangular $(8, 4)$ code. The word "rectangular" refers to the encoding procedure, the manner in which message words are changed into codewords. Suppose the message word is $m = abcd \in \mathbb{F}^4$, i.e., each of a, b, c, d is 0 or 1. Arrange a, b, c, d into a 2×2 square that is the top left part of a 3×3 square and fill in the entries labelled w, x, y, z in the square

$$\begin{matrix} a & b & w \\ c & d & x \\ y & z & * \end{matrix}$$

so that the sum of the entries in each of the top two rows and in the left-most two columns is zero. Then encode by

$$abcd \mapsto abcdxyzw.$$

For example, to encode 1011 we use

$$\begin{matrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & * \end{matrix}$$

and send 10111001. When recipient checks that $a+b+w = c+d+x = a+c+y = b+d+z = 0$. If this is not the case an error is recognized, and one can correct the error (think about it!). This code also detects two errors (think about it!). You can also check that C, the set of code words, is a 4-dimensional subspace of $\mathbb{F}^8$. $\Diamond$

The next code is better than the previous one. Like the previous one, its message words consist of four bits, and it corrects one error and detects two errors (proofs later). However, the codewords for it consist of 7 bits rather than 8 in the previous example. Thus it is more efficient than the previous code.

Example 17.6. The Hamming $(7,4)$ code. Here the code words form a 4-dimensional subspace $C \subset \mathbb{F}_2^7$. A basis for C consists of the words

$$\begin{matrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{matrix}$$

Thus a valid code word is the sum of some of these four vectors. $\Diamond$

If $\mathbb{F}^d = \{\text{message words}\}$ it is convenient to define the encoding algorithm to be a linear map $f : \mathbb{F}^d \to \mathbb{F}^n$ given by right multiplication by a $d \times n$ matrix. of course we want f to be injective so different message words give different code words. In that case if C is the image of f, then f is an isomorphism $\mathbb{F}^d \to C$ so its inverse, the decoding algorithm, is also given by a linear map (equivalently, by multiplication by a matrix).

For the Hamming code the matrix

$$A = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

provides a linear map $f : \mathbb{F}_2^4 \to \mathbb{F}_2^7$,

$$\begin{aligned} f(\alpha_1, \dots, \alpha_4) &= (\alpha_1, \dots, \alpha_4) \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix} \\ &= (\alpha_1, \dots, \alpha_4, \alpha_2 + \alpha_3 + \alpha_4, \alpha_1 + \alpha_3 + \alpha_4, \alpha_1 + \alpha_2 + \alpha_4). \end{aligned}$$

The map f is obviously injective and the decoding algorithm $C = \mathrm{im}(f) \to \mathbb{F}_2^4$ is simply $(\beta_1, \dots, \beta_7) \mapsto (\beta_1, \dots, \beta_4)$.

Discussion. How should we choose C? For simplicity we will always work over the field $\mathbb{F}_2$. We should think of the set of message words as fixed, that is we are

given some $\mathbb{F}^d$ consisting of message words—a typical example might be $\mathbb{F}_2^8$, a vector space with 256 elements, which is large enough to provide a vector for each letter of the english alphabet, both upper case and lower case, a vector for each digit 0-9, and for various other everyday symbols. We are then free to choose $n > d$ and a d-dimensional subspace C of $\mathbb{F}^n$. We do not want n too big because this increases transmission time (a single message word consists of d digits but we must send n digits). However, we want C to be sort of well spread out in $\mathbb{F}^n$ so that if, for example, a single digit of a code word c is altered during transmission the received word w is not in C but c is the element of C that is closest to w. We obviously need a notion of distance for "closest" to make sense.

17.1. **Hamming distance and weight.** Let $u, v \in \mathbb{F}^n$. The Hamming distance between u and v is

$$d(u, v) := \text{the number of positions where } u \text{ and } v \text{ differ.}$$

Explicitly, if $u = (u_1, \dots, u_n)$ and $v = (v_1, \dots, v_n)$, then

$$d(u, v) = \big|\{i \mid u_i \neq v_i\}\big|.$$

The Hamming weight of $v \in \mathbb{F}^n$ is $W(v) :=$ *the number of ones in* v.

The next result shows that the Hamming distance has various good properties that justify our using the word *distance*: part (3) is called the *Triangle Inequality*—in some sense it says that the shortest distance between two points is a "straight line."; part (4) says that the Hamming distance respects the vector space structure on $\mathbb{F}^n$.

Lemma 17.7. *Let $u, v \in \mathbb{F}^n$ and let $d(-,-)$ denote the Hamming distance.*

(1) $d(v, u) = d(u, v) = W(u - v)$;
(2) $d(u, v) = 0$ *if and only if* $u = v$;
(3) $d(u, v) \leq d(u, z) + d(z, v)$ *for all* $z \in \mathbb{F}^n$;
(4) $d(u, v) = d(u + z, v + z)$ *for all* $z \in \mathbb{F}^n$.

Proof. (1) This is clear because the i^{th} entries, u_i and v_i, of u and v differ if and only if $u_i - v_i = 1$.

(2) This follows at once from (1).

(3) Fix $z = (z_1, \dots, z_n) \in \mathbb{F}^n$. If $u_i \neq v_i$, then either $u_i \neq z_i$ or $v_i \neq z_i$.

(4) We have $d(u + z, v + z) = W((u + z) - (v + z)) = W(u - v) = d(u, v)$. □

If a codeword u is transmitted and v is received the number of errors in transmission is the number of coordinates in which u and v differ; that is, $d(u, v)$.

The next result says that if the probability that an error occurs when transmitting a single digit (bit) is small, then it is more probable that few rather than many errors occur in transmission. We shall always make this assumption.

Proposition 17.8. *Let p denote the probability that an error occurs when transmitting a single digit (bit). Let $P(t, n)$ denote the probability that t errors occur when transmitting $n \geq 1$ digits. If $p < \frac{1}{n+1}$, then*

$$(1 - p)^n = P(0, n) > P(1, n) > P(2, n) > \cdots > P(n - 1, n) > P(n, n) = p^n.$$

Proof. There are $\binom{n}{t}$ ways in which exactly t errors can occur when transmitting n digits, so

$$P(t, n) = \binom{n}{t} p^t (1 - p)^{n-t}.$$

Therefore

$$\frac{P(t+1,n)}{P(t,n)} = \frac{n!}{(t+1)!(n-t-1)!} \cdot \frac{t!(n-t)!}{n!} \cdot \frac{p}{1-p} = \frac{n-t}{t+1} \cdot \frac{p}{1-p}.$$

We want to show that this is < 1. The hypothesis is that $(n+1)p < 1$, so $(n-t+t+1)p < t+1$ for all $t = 0, 1, \ldots, n$, and this can be rewritten as $(n-t)p < (t+1)(1-p)$, from which the result follows. □

17.2. **Nearest neighbor decoding.** Proposition 17.8 shows that if $p < \frac{1}{n+1}$ it is more likely that there are fewer rather than more errors so *the codeword nearest to a received word is most likely the codeword that was transmitted*. We therefore adopt the following decoding policy:

- *a received word is decoded as the codeword nearest to it and*
- *if there is more than one codeword nearest to a received word the decoder records an error.*

We call this (maximum-likelihood) nearest neighbor decoding.

We say that a linear code

- corrects t errors if every codeword that is transmitted with $\leq t$ errors is correctly decoded by nearest neighbor decoding.
- detects $2t$ errors if a codeword cannot be changed to a different codeword by changing $\leq 2t$ bits.

17.3. **Balls.** Let $v \in \mathbb{F}^n$ and t a non-negative number (usually a positive integer). The ball of radius t with center v is

$$B_t(v) := \{z \in \mathbb{F}^n \mid d(v,z) \leq t\}.$$

Proposition 17.9. *Let $u, v \in \mathbb{F}^n$ and s and t non-negative integers. Then*

$$B_s(u) \cap B_t(v) \neq \phi \quad \Longleftrightarrow \quad d(u,v) \leq s+t.$$

Proof. ($\Rightarrow$) If z belongs to both balls, then $d(u,v) \leq d(u,z) + d(z,v) \leq s+t$.

($\Leftarrow$)[1] If $d(u,v) \leq s$, then the balls intersect because v is in both. If $s \leq d(u,v) \leq s+t$, then we can change s digits of u that differ from the corresponding digits in v to get an element z; clearly $d(u,z) = s$ and $d(z,v) \leq t$, so z is in both balls. □

It is easier to detect errors than correct them—we saw this with the ISBNs where one could recognize a non-ISBN but not know which ISBN it was "trying to be". A linear code $C \subset \mathbb{F}^n$ detects t errors if and only if $d(u,v) \geq t+1$ for all $u \neq v$ in C.

Lemma 17.10. *The following conditions on a linear code C are equivalent:*

(1) *C corrects t errors;*
(2) *for all $u \in C$ and all $z \in B_t(u)$, u is the unique element of C having distance $\leq t$ from z;*
(3) *$B_t(u) \cap B_t(v) = \phi$ whenever u and v are distinct elements of C;*
(4) *$\min\{W(u) \mid 0 \neq u \in C\} \geq 2t+1$.*

Proof. Better you convince yourself than read what I write. □

[1]The implication ($\Rightarrow$) is true for any pair of non-negative real numbers s and t. But the implication ($\Leftarrow$) fails if s and t are not integers: for example, if $d(u,v) = 1$, and s and t are positive numbers such that $s+t = 1$, then the intersection of the balls is empty.

Theorem 17.11. *The following conditions on a linear code C are equivalent:*

(1) *C corrects t errors;*
(2) *$d(u,v) \geq 2t+1$ for all $u \neq v$ in C;*
(3) *$W(u) \geq 2t+1$ for all $0 \neq u \in C$.*

Proof. This follows from the previous two results. □

17.4. **(n,k,d) linear codes.** An (n,k,d)-code is an (n,k)-linear code such that

$$d = \min\{W(u) \mid 0 \neq u \in C\}.$$

In other words, distinct codewords are distance at least d apart and there are code words exactly distance d apart.

Corollary 17.12. *An (n,k,d) code corrects t errors and detects $2t$ errors if and only if $d \geq 2t+1$.*

Proof. This is a restatement of Theorem 17.11. □

Lemma 17.13. *Let $\mathbb{F}^k \cong C \subset \mathbb{F}^n$ be an (n,k)-linear code.*

(1) *If C is is an (n,k,d)-code, then the balls $B_{\frac{d-1}{2}}(u)$, $u \in C$, are disjoint.*
(2) *If c is the largest integer such that the balls $B_c(u)$, $u \in C$, are disjoint then the minimum distance for the code is either $2c+1$ or $2c+2$.*

Proof. (1) If z were in two distinct such balls, say those centered at $u, v \in C$, then $d(u,v) \leq d(u,z) + d(z,v) = d-1$, so the minimum distance would be $\leq d-1$.

(2) By Proposition 17.9, the fact that $B_c(u) \cap B_c(v) = \phi$ implies that $d(u,v) > 2c$, and hence is $\geq 2c+1$. However, if the minimum distance were $\geq 2c+3$, Proposition 17.9 would imply that the balls $B_{c+1}(u)$, $u \in C$, were disjoint, contradicting the choice of c. □

17.5. **Perfect codes.** If $a \in \mathbb{R}$ we define $[a] :=$ the largest integer that is $\leq a$.

An (n,k,d)-code $\mathbb{F}^k \cong C \subset \mathbb{F}^n$ is perfect if $\mathbb{F}^n$ is the disjoint union of the balls $B_t(u)$, $u \in C$, where $t = \left[\frac{d-1}{2}\right]$.

Proposition 17.14. *An (n,k,d) code $C \subset \mathbb{F}^n$ is perfect if and only if*

$$2^{n-k} = 1 + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{t} \tag{17-1}$$

where $t = \left[\frac{d-1}{2}\right]$.

Proof. Fix $u \in \mathbb{F}^n$. The number of elements in $\mathbb{F}^n$ that differ from u in exactly $i \leq n$ positions is $\binom{n}{i}$ so the number of elements in $B_t(u)$ is

$$\sum_{i=0}^{t} \binom{n}{i} = 1 + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{t}.$$

($\Rightarrow$) There are 2^n elements in $\mathbb{F}^n$ and 2^k elements in C, so if $\mathbb{F}^n$ is the disjoint union of the balls $B_t(u)$, $u \in C$, then

$$2^n = 2^k\left(1 + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{t}\right). \tag{17-2}$$

($\Leftarrow$) Since $W(u) \geq d \geq 2t+1$ for $0 \neq u \in C$, the balls $B_t(u)$, $u \in C$, are disjoint. Therefore the number of elements in their union is the right-hand side of (17-2) which equals 2^n by hypothesis. Hence the union of the balls is equal to $\mathbb{F}_2^n$. □

Warning: Proposition 17.14 does *not* say that a perfect (n, k, d) code exists if the equation (17-1) holds. However, if there is an (n, k, d)-code such that equation (17-1) holds then that code must be perfect. Let's look for some perfect codes.

17.6. **Perfect 1-error correcting codes.** This is the simplest case. By Corollary 17.12, $(n, k, 3)$-code corrects 1 error and detects 2 errors. An $(n, k, 3)$ code is perfect if and only if

$$2^{n-k} = 1 + \binom{n}{1} = n + 1$$

so our search for a perfect $(n, k, 3)$-code must begin by taking n to be one less than a power of two.

• A perfect code with $n = 1$ would be useless because then k would be zero so $\mathbb{F}^k = \{0\}$ and the only message word is 0, and C is the zero subspace of $\mathbb{F}^n$. Such a code can only send one message, a string of zeroes, duh! So, the first interesting case of a 1-error correcting code would be when $n = 3$, and $k = 1$.

• There is a perfect $(3, 1, 3)$-code. Let $C \subset \mathbb{F}^3$ be the subspace $\{000, 111\}$. This is a perfect $(3, 1, 3)$-code. The isomorphism $\mathbb{F} = \mathbb{F}^k \to C$ is given by $0 \mapsto 000$ and $1 \mapsto 111$. The message words are the elements of $\mathbb{F}$, namely $\{0, 1\}$, and the corresponding code words are 000 and 111. This code triples the length of a message; it detects two errors and corrects one error.

• The next smallest n for which a perfect $(n, k, 3)$-code might exist is $n = 2^3 - 1 = 7$. In this case k must be 4.

Proposition 17.15. *The Hamming* $(7, 4)$*-code is a perfect* $(7, 4, 3)$*-code.*

Proof. We must check that all non-zero codewords have weight ≥ 3 and at least one code word has weight exactly 3. A basis for C is given by

$$a = 1000011,\ b = 0100101,\ c = 0010110,\ d = 0001111.$$

The non-zero elements of C written in "alphabetical order", namely

$$a,\ ab,\ abc,\ abcd,\ abd,\ ac,\ acd,\ ad,\ b,\ bc,\ bcd,\ bd,\ c,\ cd,\ d,$$

where acd denotes $a + c + d$, et cetera, are

1000011, 1100110, 1110000, 1111111, 1101010, 1010101, 1011010, 1001100,

0100101, 0110011, 0111100, 0101010, 0010110, 0011001, 0001111.

Since each of these has weight ≥ 3, we are done. □

The next smallest n for which a perfect $(n, k, 3)$ code might exist is $n = 2^4 - 1 = 15$ and $k = 11$. Is there a perfect $(15, 11, 3)$ code?

17.7. **Perfect 3-error correcting codes.** An $(n, k, 7)$-code is 3-error correcting and will be perfect if and only if

$$1 + \binom{n}{1} + \binom{n}{2} + \binom{n}{3} = 2^{n-k}.$$

A calculation with $n = 23$ gives

$$1 + \binom{23}{1} + \binom{23}{2} + \binom{23}{3} = 2048 = 2^{11} = 2^{23-12}$$

so a $(23, 12, 7)$-code will be perfect if it exists. How can we find one or decide one does not exist. This is a hard question. There is one, and it is due to Golay. It is

intimately related to a sporadic simple group, the Mathieu group M_{24}. It is also related to the most efficient known packing of spheres in 24-dimensional space. See http://www.math.uic.edu/ fields/DecodingGolayHTML/introduction.html

In 1949, Golay published a half-page article *Notes on digital coding* in the Proceedings of the Institute of Electrical and Electronic Engineers that is now seen as one of the most important publications of the last century. Today, reliable data transmission uses methods developed from that original article.

17.8. **Further remarks.** Other important codes are the Golay $(11, 6, 5)$-code, and the Reed-Muller $(32, 6, 16)$ code. The latter was used on the Mariner 6, 7, and 9 voyages to transmit pictures back to earth. Each picture consisted of 700×832 pixels, each of which had $64 = 2^6$ brightness levels black-white. The cameras produced pictures at the rate of 100,000 bits per second but data could be transmitted back to earth only at 16,200 bps, so pictures were temporarily stored on tape prior to transmission. For this reason the question of efficiency is of great importance in constructing codes. The Reed-Muller code corrects 7 errors; thus if 7/32, or a little over 22%, of a code word is corrupted in transmission one can still determine the original code word.

The Voyager 1 and Voyager 2 spacecraft transmitted color pictures of Jupiter and Saturn in 1979 and 1980. Color image transmission required 3 times the amount of data, so the Golay (24,12,8) code was used (this is a jazzed up version of his $(23, 12, 7)$ code). This Golay code is only 3-error correcting, but could be transmitted at a much higher data rate than the Reed-Muller code because $\frac{23}{12}$ is much smaller than $\frac{32}{6}$. Voyager 2 went on to Uranus and Neptune and the code was switched to a Reed-Solomon code.

In 1960, Reed and Solomon introduced their codes in a five-page article "Polynomial Codes over Certain Finite Fields," in the Journal of the Society for Industrial and Applied Mathematics. The basic idea is this. Let $n = 2^r$ and take $k < n$. (A typical example is $r = 8$). Let $K = \mathbb{F}_n$ and choose a generator, say α, for the cyclic group $K - \{0\}$. Given a message word $m = a_0a_1a_2 \cdots a_{k-1} \in K^k$ form the polynomial $f = a_0 + a_1x + a_2x^2 + \cdots + a_{k-1}x^{k-1} \in K[x]$ and evaluate it at each element of K to obtain a code word

$$F(m) := (f(0), f(\alpha), f(\alpha^2), \dots, f(\alpha^{n-1})) \in K^n.$$

Since f is a polynomial of degree $\leq k-1$ we can determine it once we know its value at k different points. Since $n > k$, we can recover f, and hence its coefficients which are the message word, from the code word. The idea behind the error correction is this. If you plot some points on the graph of a polynomial, for arguments sake let's say 20 points of a degree 4 polynomial, and a small number of those points are incorrect one can "see" that by looking at the graph and still figure out what the polynomial is that is being corrected.

The 2004 missions to Mars and Saturn transmitted photographs consisting of 1024×1024 and each pixel consisted of a 12 bits giving its color, brightness, intensity, etc. Thus each picture required $2^{10} \times 2^{10} \times 12$ bits. That is a little more than 12 million bits per photograph.

Error-correcting codes are essential for computer disk drives, CD players, television transmissions, phone calls, and all kinds of data transmission over both short and long distances. Careful engineering can reduce the error rate to what may sound like a negligible level–the industry standard for hard disk drives is 1 in 10

billion–but given today's volume of information processing that "negligible" level is an invitation to disaster. Billions and billions of dollars of equipment and millions of lives depend on error correcting codes. The world would look very different without these ideas, all of which grow out of elementary abstract algebra. The abstract algebra on which coding theory rests was developed over the last 150 years which was in turn developed to answer questions and problems that had arisen from within mathematics over the two or three centuries prior to that. In particular, none of this mathematics was developed with the goal of being used in the real world. Keep this in mind the next time you hear about cutting the budget for the National Science Foundation because the research being done is "of no practical use."

18. BCH codes

These codes were invented by Bose, Chauduri, and Hocquenghem. The following definition is vague but will tell you where we are headed.

Definition 18.1. A BCH code is a linear code of the form

$$C = \frac{(g)}{(x^n-1)} \subset \frac{\mathbb{F}[x]}{(x^n-1)} \cong \mathbb{F}^n$$

where $g \in \mathbb{F}[x]$ is a (carefully chosen) polynomial dividing $x^n - 1$. ◊

18.1. **Notation.** We will write elements of $\mathbb{F}[x]/(x^n-1)$ as truncated polynomials of degree $\leq n-1$. For example, in $\mathbb{F}[x]/(x^7-1)$ we have

$$(1+x^2+x^4)(1+x^3+x^4+x^6) = 1+x^3+x^4+x^6+x^2+x^5+x^6+x+x^4+1+x+x^3 = x+x^2+x^5.$$

We will adopt $1, x, x^2, \ldots, x^{n-1}$ as a basis for $\mathbb{F}[x]/(x^n-1)$ and write $(a_0, a_1, \ldots, a_{n-1})$ for the polynomial $a_0+a_1x+\cdots+a_{n-1}x^{n-1} \in \mathbb{F}[x]/(x^n-1)$. Hence, when we speak of the weight of an element in $\mathbb{F}[x]/(x^n-1) \cong \mathbb{F}^n$ we mean its weight with respect to this basis, i.e., the number of non-zero coefficients/entries in $(a_0, a_1, \ldots, a_{n-1}) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1}$.

18.2. **The recipe for a BCH code.** Choose integers t, r with $t < 2^r - 1$ and write $n = 2^r-1$. We will construct an (n, k, d) linear code where $d \geq 2t+1$. It will detect $2t$ errors and correct t errors. The code is constructed in 3 steps.

(1) Let $K = \mathbb{F}_{2^r}$ be the field with 2^r elements. Fix some $\alpha \in K$ such that
$$K = \{0\} \cup \{\alpha, \alpha^2, \ldots, \alpha^n = 1\}.$$
Such an α exists by Theorem 16.4.

(2) The minimal polynomial of $\beta \in K$ is the non-zero polynomial $m \in \mathbb{F}[x]$ of smallest degree such that $m(\beta) = 0$. Compute the minimal polynomials of $\alpha, \alpha^2, \ldots, \alpha^{2t}$, and write m_i for the minimal polynomial of α^i. Define
$$g = \operatorname{lcm}\{m_1, \ldots, m_{2t}\}.$$

(3) The BCH code of length n and designated distance $2t+1$ is
$$C = \frac{(g)}{(x^n-1)} \subset \frac{\mathbb{F}[x]}{(x^n-1)}.$$
We will show that g divides $x^n - 1$ in section 18.4 so that (g) *does* contain $(x^n - 1)$.

Theorem 18.2. *The minimum distance of this BCH code is* $\geq 2t+1$.

We will prove this in subsection 18.6.

18.3. **Minimal polynomials.**

Lemma 18.3. *Let $k \subset K$ be fields such that $\dim_k K < \infty$. Let $m \in k[x]$ be the minimal polynomial of an element $\beta \in K$. Then m is irreducible.*

Proof. Since $\dim_k K < \infty$, the powers $1, \beta, \beta^2, \dots$ are linearly dependent. Hence there is a non-zero polynomial f such that $f(\beta) = 0$. Let m be the minimal polynomial. If $m = gh$, then $0 = m(\beta) = g(\beta)h(\beta)$ so either $g(\beta) = 0$ or $h(\beta) = 0$. It follows that m is irreducible. □

We have seen many times that if a and b belong to a field of characteristic p, then $(a+b)^p = a^p + b^p$. It follows from this that if f is a polynomial with coefficients in K, then $f(a^p) = f(a)^p$.

Lemma 18.4. *Let $k \subset K$ be fields such that $\dim_k K < \infty$. Let $m \in k[x]$ be the minimal polynomial of an element $\beta \in K$. If the characteristic of K is p, then m is also the minimal polynomial of $\beta^p, \beta^{p^2}, \dots$.*

Proof. If $f \in k[x]$, then $f(\beta)^p = f(\beta^p)$, so $f(\beta) = 0$ if and only if $f(\beta^p) = 0$. Hence β and β^p have the same minimal polynomial. The other cases are similar. □

18.4. **The g defined in section ?? divides $x^n - 1$.** Because the multiplicative group $(K\backslash\{0\}, \cdot)$ has order $n = 2^r - 1$, the order of every element in it divides n. In other words, $x^n - 1$ vanishes on all n elements of $K\backslash\{0\}$. Since $x^n - 1$ is in the kernel of the evaluation map $f \mapsto f(\beta)$, the minimal polynomial of every $0 \neq \beta \in K$ divides $x^n - 1$.

Hence the least common multiple of all such minimal polynomials must divide $x^n - 1$.

18.5. **A $(15, 7, 5)$-code.** Here $n = 2^4 - 1 = 15$, $r = 4$, and $t = 2$. We realize $K = \mathbb{F}_{16}$ as

$$K = \frac{\mathbb{F}[t]}{(t^4 + t + 1)}.$$

The irreducibility of $t^4 + t + 1$ ensures that K is a field; to see that $t^4 + t + 1$ is irreducible, observe that it has no linear factors because it has no zeroes in $\mathbb{F} = \mathbb{F}_2$, and it has no quadratic factors because the only degree two irreducible is $t^2 + t + 1$ and $t^4 + t + 1 \neq (t^2 + t + 1)^2$.

Let $\alpha = [t]$ denote the image of t in K. Straightforward computations give

	$\alpha^4 = \alpha + 1$	$\alpha^8 = \alpha^2 + 1$	$\alpha^{12} = \alpha^3 + \alpha^2 + \alpha + 1$
$\alpha = \alpha$	$\alpha^5 = \alpha^2 + \alpha$	$\alpha^9 = \alpha^3 + \alpha$	$\alpha^{13} = \alpha^3 + \alpha^2 + 1$
$\alpha^2 = \alpha^2$	$\alpha^6 = \alpha^3 + \alpha^2$	$\alpha^{10} = \alpha^2 + \alpha + 1$	$\alpha^{14} = \alpha^3 + 1$
$\alpha^3 = \alpha^3$	$\alpha^7 = \alpha^3 + \alpha + 1$	$\alpha^{11} = \alpha^3 + \alpha^2 + \alpha$	$\alpha^{15} = 1$

Let's write m_i for the minimal polynomial of α^i. We want to find $g \in \mathbb{F}[x]$, the least common multiple of $m_1, m_2, \dots, m_4 = m_{2t}$.

By definition of α, it is a zero of $x^4 + x + 1$ which is irreducible, so

$$m_1 = x^4 + x + 1.$$

Because we are working over a field of characteristic two, this is also the minimal polynomial of $\alpha^2, \alpha^4, \alpha^8$, so $m_1 = m_2 = m_4$.

To find m_3, the minimal polynomial of α^3, notice that m_3 is also the minimal polynomial of $\alpha^6, \alpha^{12}, \alpha^{24} = \alpha^9$, so

$$\begin{aligned} m_3(x) &= (x-\alpha^3)(x-\alpha^6)(x-\alpha^9)(x-\alpha^{12}) \\ &= (x^2-(\alpha^3+\alpha^6)x+\alpha^9)(x^2-(\alpha^9+\alpha^{12})x+\alpha^6) \\ &= x^4-(\alpha^3+\alpha^6+\alpha^9+\alpha^{12})x^3+\cdots \\ &= x^4+x^3+x^2+x+1. \end{aligned}$$

Hence

$$g(x) = (x^4+x+1)(x^4+x^3+x^2+x+1) = x^8+x^7+x^6+x^4+1.$$

Hence the BCH code is

$$\mathbb{F}^7 \cong C = \frac{(g = x^8+x^7+x^6+x^4+1)}{(x^{15}-1)} \subset \frac{\mathbb{F}[x]}{(x^{15}-1)} \cong \mathbb{F}^{15}.$$

Notice that the weight of the code word g is 5. To verify our claim that this is a $(15,7,5)$-code we must show that every multiple of g, gh with $\deg h \leq 8$, has at least five non-zero coefficients. There are 2^8-1 such $h's$ so we surely do not want to do this by checking every case. The result is Theorem 18.2, which we now prove.

18.6. **Proof of Theorem 18.2.** We must show that a non-zero codeword has weight $\geq 2t+1$. In other words we must show that at least $2t+1$ coefficients of a non-zero

$$f = a_0 + a_1x + \cdots + a_{n-1}x^{n-1} \in (g)$$

are non-zero. Suppose to the contrary that the number of non-zero a_js is $d \leq 2t$.

Since f is a multiple of the minimal polynomial of α^i, $1 \leq i \leq 2t$, Let $a_{j_1}, \ldots, a_{j_d}$ be the non-zero coefficients of f. $f(\alpha^i) = 0$ for $1 \leq i \leq 2t$. We can express this as the matrix equation

$$\begin{pmatrix} a_0 & a_1 & \ldots & a_{n-1} \end{pmatrix} \begin{pmatrix} 1 & 1 & \ldots & 1 \\ \alpha & \alpha^2 & \ldots & \alpha^{2t} \\ \alpha^2 & \alpha^4 & \ldots & \alpha^{4t} \\ \vdots & & & \vdots \\ \alpha^{n-1} & \alpha^{2(n-1)} & \ldots & \alpha^{2t(n-1)} \end{pmatrix} = 0.$$

Let $a_{j_1}, \ldots, a_{j_d}$ be the non-zero coefficients of f. Taking the submatrix consisting of the first d columns and the rows labelled $j_1, \ldots, j_d$ we obtain

$$\begin{pmatrix} a_{j_1} & \ldots & a_{j_d} \end{pmatrix} \begin{pmatrix} \alpha^{j_1} & \alpha^{2j_1} & \ldots & \alpha^{dj_1} \\ \alpha^{j_2} & \alpha^{2j_2} & \ldots & \alpha^{dj_2} \\ \vdots & & & \vdots \\ \alpha^{j_d} & \alpha^{2j_d} & \ldots & \alpha^{dj_d} \end{pmatrix} = 0.$$

It follows that the determinant of this $d \times d$ matrix is zero. However, that determinant is

$$\alpha^{j_1+\cdots+j_d} \begin{pmatrix} 1 & \alpha^{j_1} & (\alpha^{j_1})^2 & \ldots & (\alpha^{j_1})^{d-1} \\ 1 & \alpha^{j_2} & (\alpha^{j_2})^2 & \ldots & (\alpha^{j_2})^{d-1} \\ \vdots & & & \vdots & \\ 1 & \alpha^{j_d} & (\alpha^{j_d})^2 & \ldots & (\alpha^{j_d})^{d-1} \end{pmatrix} = 0.$$

However, it follows from the next lemma that there are two different values of i for which α^{j_i} are the same; this contradicts the fact that α^i, $1 \leq i \leq n$ are distinct. We conclude that the number of non-zero a_js must be $\geq 2t+1$.

18.7. **The Vandermonde determinant.**

Lemma 18.5. *If $f(x_1, \ldots, x_n)$ is an alternating homogeneous polynomial of degree $\frac{1}{2}n(n-1)$, then*

$$f(x_1, \ldots, x_n) = c\prod_{i<j}(x_i - x_j)$$

for some $c \in k$.

Proof. To say that f is alternating means that the value of f changes by a sign if the position of two of the variables is switched:

$$f(x_1, \ldots, x_j, \ldots, x_i, \ldots, x_n) = -f(x_1, \ldots, x_i, \ldots, x_j, \ldots, x_n).$$

Write f as a polynomial in x_1 and x_2 with coefficients in $k[x_3, \ldots, x_n]$, say

$$f = \sum_{i,j} a_{ij} x_1^i x_2^j.$$

The alternating hypothesis says that

$$\sum_{i,j} a_{ij} x_1^j x_2^i = -\sum_{i,j} a_{ij} x_1^i x_2^j$$

so $a_{ij} = -a_{ji}$ and we can now write

$$f = \sum_{i<j} a_{ij}(x_1^i x_2^j - x_1^j x_2^j).$$

However, there is a factorization

$$\begin{aligned} x^i y^j - x^j y^i &= x^i y^j \left(1 - \left(\frac{x}{y}\right)^{j-i}\right) \\ &= x^i y^j \left(1 - \frac{x}{y}\right)\left(1 + \left(\frac{x}{y}\right) + \cdots + \left(\frac{x}{y}\right)^{j-i-1}\right) \\ &= (y-x)x^i(y^{j-1} + xy^{j-2} + \cdots + x^{j-i-1}y^i) \end{aligned}$$

so we can write $x_1^i x_2^j - x_1^j x_2^i = (x_1 - x_2)g$ for some polynomial $g \in k[x_1, x_2]$. Hence f is divisible by $x_1 - x_2$. We can repeat this argument for every pair of variables x_i and x_j to see that $x_i - x_j$ divides f. It follows that f is a multiple of the product

$$\prod_{i<j}(x_i - x_j)$$

of those factors. This product has $\binom{n}{2}$ terms so has the same degree as f. The result follows. □

Theorem 18.6. *The following formula holds for the determinant:*

$$\det \begin{pmatrix} 1 & 1 & \ldots & 1 \\ x_1 & x_2 & \ldots & x_n \\ x_1^2 & x_2^2 & \ldots & x_n^2 \\ \vdots & & & \vdots \\ x_1^{n-1} & x_2^{n-1} & \ldots & x_n^{n-1} \end{pmatrix} = \prod_{i<j}(x_i - x_j).$$

Proof. Write $f(x_1, \ldots, x_n) = \det A$ for the determinant of this matrix; it is a polynomial in $x_1, \ldots, x_n$. Since the determinant is a sum of products, and each product is the product of a single term from each row, each term of $f = \det A$ has degree

$$0 + 1 + 2 + \cdots + (n-1) = \frac{1}{2}n(n-1) = \binom{n}{2}.$$

Because the determinant changes sign when two columns are switched, f is an alternating function. Now the only such polynomials are the scalar multiples of $\prod_{i<j}(x_i - x_j)$. However, by multiplying the diagonal terms, we see that the coefficient of $x_1 x_2^2 \ldots x_n^{n-1}$ is one. So the multiple must be one. □

19. Implementing nearest neighbor decoding

Dot product on $\mathbb{F}^n$. There is a dot product in $\mathbb{F}^n$, namely

$$u \cdot v := \sum_{i=1}^{n} u_i v_i$$

where $u = (u_1, \ldots, u_n)$ and $v = (v_1, \ldots, v_n)$. We say that u and v are orthogonal if $u \cdot v = 0$. We write

$$u^\perp := \{v \in \mathbb{F}^n \mid u \cdot v = 0\}.$$

If u is non-zero, $u^\perp$ is a subspace of dimension one; this is because the map $v \mapsto u \cdot v$ is a surjective linear map $\mathbb{F}^n \to \mathbb{F}$ (see Theorem 15.8). More generally, if D is any subset of $\mathbb{F}^n$ we define

$$D^\perp := \{v \in \mathbb{F}^n \mid u \cdot v = 0 \text{ for all } u \in D\};$$

this is a subspace of $\mathbb{F}^n$.

Let $e_1, \ldots, e_n$ be the usual basis for $\mathbb{F}^n$, i.e., e_i has a 1 in the i^{th} position and zeroes elsewhere. Then

$$e_i \cdot e_j = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{if } i \neq j. \end{cases}$$

More about the Hamming $(7, 4, 3)$-code. Let $\mathbb{F}^4 \cong C \subset \mathbb{F}^7$ be the Hamming code. Claim: The vectors

$$x = 0001111,\ y = 0110011,\ z = 1010101$$

belong to $C^\perp$. To verify this it suffices to check that x, y, and z are othogonal to a set of basis vectors for C. Now C was defined to be the linear span of the elements

$$a = 1000011,\ b = 0100101,\ c = 0010110,\ d = 0001111$$

It is routine to verify that x, y, z are orthogonal to a, b, c, d. Define the matrices

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}, \qquad E = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix}.$$

The orthogonality can now be expressed as saying that $GE = 0$. Since E is a 3×7 matrix it gives a linear map $\mathbb{F}^7 \to \mathbb{F}^3$, $u \mapsto uE$. Now G is the encoding matrix in the sense that the linear map $\mathbb{F}^4 \to \mathbb{F}^7$ given by $v \mapsto vG$ encodes the message words as code words. It is easy to see that the map $\mathbb{F}^7 \to \mathbb{F}^3$, $u \mapsto uE$ is surjective (because the rows of E span $\mathbb{F}^3$). By Theorem 15.8, the kernel of this map therefore has dimension four; but the kernel contains C which is 4-dimensional, so the kernel is exactly C. In other words, $u \in C \Leftrightarrow uE = 0$; thus E provides a way of checking whether the received word is a valid code word.

The next lemma shows that E does an awful lot more than that.

Lemma 19.1. *Consider the Hamming $(7, 4, 3)$-code $\mathbb{F}^4 \cong C \subset \mathbb{F}^7$. Suppose that a code word u is transmitted and an error occurs in the i^{th} digit, so that $v = u + e_i$ is received. Then vE is the binary representation of the number e_i. Thus vE tells us exactly which digit is wrong.*

Proof. Now $vE = (u + e_i)E = uE + e_iE = e_iE$, so we simply need to check that for the seven basis vectors $e_i \in \mathbb{F}^7$, e_iE is the binary representation of the integer i, $i = 1, \ldots, 7$. Now e_iE is equal to the i^{th} row of E. Since the i^{th} row of E is indeed the binary representation of the integer i the result follows. □

If you need more convincing try a few examples—impress your friends and family: let them pick any element u of C, change one digit, and you then tell them which digit they changed!

All this is capable of generalization. Observe that G is of the form $(I_4 \,|\, A)$ where I_4 is the 4×4 identity matrix and A is a 4×3 matrix. We call a $k \times n$ matrix of the form $G = (I_k \,|\, A)$ a standard generator matrix. The map $\mathbb{F}^k \to \mathbb{F}^n$, $v \mapsto vG$, is injective, so its image C is isomorphic to $\mathbb{F}^k$. Thus G gives rise to an (n, k)-linear code, $\mathbb{F}^k \cong C = \{vG \mid v \in \mathbb{F}^k\} \subset \mathbb{F}^n$.

Theorem 19.2. *Let $G = (I_k \,|\, A)$ be a $k \times n$ standard generator matrix and define the $n \times k$ matrix*

$$H = \begin{pmatrix} A \\ \hline I_{n-k} \end{pmatrix}.$$

Then $GH = 0$ and for each $w \in \mathbb{F}^n$,

1. *$wH = 0$ if and only if $w \in C := \{vG \mid v \in \mathbb{F}^k\}$;*
2. *if $e \in \mathbb{F}^n$ is the smallest weight word such that $wH = eH$, then the rule $w \mapsto w - e$ is nearest neighbor decoding.*

Proof. We use the notation

$$\delta_{ij} = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{if } i \neq j. \end{cases}$$

Notice that A is a $k \times (n-k)$ matrix. Let's write $A = (a_{ij})_{1 \le i \le k,\, 1 \le j \le n-k}$. The ij-entry of GH is the product of the i^{th} row of G with the j^{th} column of H, namely

$$\begin{pmatrix} \delta_{i1} & \cdots & \delta_{ik} & a_{i1} & \cdots & a_{i\,n-k} \end{pmatrix} \begin{pmatrix} a_{1j} \\ \vdots \\ a_{kj} \\ \delta_{1j} \\ \vdots \\ \delta_{n-k\,j} \end{pmatrix} = a_{ij} + a_{ij} = 0.$$

Hence $GH = 0$.

(1) Let $\phi : \mathbb{F}^n \to \mathbb{F}^{n-k}$ be the linear map $\phi(w) = wH$. Because the identity matrix I_{n-k} appears in the lower part of H, ϕ is surjective. But

$$n = \dim \mathbb{F}^n = \dim(\operatorname{im} \phi) + \dim(\ker \phi)$$

so $\dim(\ker \phi) = k$. However, since $GH = 0$, and C is the image of the map $\mathbb{F}^k \to \mathbb{F}^n$, $v \mapsto vG$, $C \subset \ker \phi$. Since C and $\ker \phi$ have the same dimension they are equal. Thus $wH = 0$ if and only if $w \in C$.

(2) We must show that $w - e$ is the codeword that is nearest to w. First, $w - e$ is a codeword because $(w-e)H = 0$. Notice that $\{v \in \mathbb{F}^n \mid vH = wH\} = w + C$; in particular, this is a coset of C. Thus, e is the element in $w + C$ of minimal weight. If u is a code word, then $w - u \in w + C$, so $W(w-u) \ge W(e)$. Hence

$$d(w,u) = W(w-u) \ge W(e) = d(w, w-e).$$

Hence u is no closer to w than $w - e$ is. □

We call the H in Lemma 19.2 the parity check matrix for the code generated by G.

Here is one way to implement this decoding algorithm.

(1) Find an element in each coset $w + C$, $w \in \mathbb{F}^n$, of minimal weight. Call this a coset leader. The cosets are the elements of $\mathbb{F}^n/C \cong \mathbb{F}^{n-k}$, so there are 2^{n-k} different coset leaders.
(2) Create a table of elements $eH \in \mathbb{F}^{n-k}$, one for each coset leader e.
(3) If w is received, compute wH, then look at the table to find the e such that $eH = wH$.
(4) Decode w as $w - e$.

Warning. Coset leaders are not necessarily unique: there might be several elements in a given coset $w + C$ having the same minimal weight. For example, if $e_i + e_j$ is a code word, then $e_i + C = e_j + C$, so either e_i or e_J could be chosen as a coset leader for $e_i + C$.

We call wH the syndrome of w. The table we create is called a syndrome look-up table. Here is what it is for the Hamming code.

Syndrome	Coset leader
000	0000000
001	0000001=e_7
010	0000010=e_6
011	1000000=e_1
100	0000100=e_5
101	0100000=e_2

110 0010000=e_3
111 0001000=e_4