1 Rings

We are familiar with

- integers $\mathbb{Z}$;
- rational numbers $\mathbb{Q}$;
- real numbers $\mathbb{R}$;
- complex numbers $\mathbb{C}$;
- $n \times n$ matrices $M_n(\mathbb{R})$ with real entries;
- integers $\mathbb{Z}_2$ modulo 2;
- polynomials $\mathbb{R}[X]$ with real coefficients;
- continuous functions $C([0,1])$ on the interval [0,1].

What are the common algebraic properties of all these sets?

Definition 1.1 A *group* $(G, *)$ is a set G together with a binary operation $*$ such that the following axioms are satisfied:

(G1) The binary operation $*$ is associative.

(G2) There is an element e in G such that $e * x = x * e = x$ for all $x \in G$. This element e is an *identity element* for $*$ on G.

(G3) For each $a \in G$, there is an element $a' \in G$ with the property that $a' * a = a * a' = e$. The element a' is an *inverse of* a *with respect to* $*$.

A group in which the binary operation is commutative, that is, $x * y = y * x$ for all x, y, is a *commutative* or *abelian group*.

Example 1.2 Some important groups.

1. The integers $\mathbb{Z}$ form a commutative group with respect to addition. However, $\mathbb{Z}$ is not a group with respect to multiplication.
2. The integers modulo n, $\mathbb{Z}_n$, form a commutative group with respect to addition modulo n.
3. The collection of all invertible $n \times n$ matrices with entries in $\mathbb{R}$ forms a group $GL(n, \mathbb{R})$ with respect to multiplication of matrices. This group is not commutative in case $n > 1$.
4. The collection of all distance preserving maps of $\mathbb{R}^2$ forms a group with respect to composition of maps.

Definition 1.3 A **ring** $(R, +, \cdot)$ is a set R together with two binary operations, addition $+$ and multiplication $\cdot$, defined on R such that the following axioms are satisfied:

(R1) $(R, +)$ is a commutative group.

(R2) Multiplication is associative.

(R3) For all $a, b, c \in R$, the **distributive laws**

$a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ and

$(a + b) \cdot c = (a \cdot c) + (b \cdot c)$

hold.

(Normally, the multiplication $\cdot$ is not written explicitly.)

A ring in which the multiplication is commutative is a **commutative ring**.

A **unity** in a ring R is a nonzero element 1 such that $1x = x1 = x$ for all $x \in R$. If such a multiplicative identity exists then R is called in a **ring with unity**.

A **multiplicative inverse** of an element a in a ring R with unity 1 is an element $a^{-1} \in R$ such that $aa^{-1} = a^{-1}a = 1$. An element u in R is a **unit of** R if it has a multiplicative inverse in R.

Example 1.4

1. $\mathbb{Z}$ is a commutative ring with unity under the usual addition and multiplication of integers, but $\mathbb{N}$ is not.
2. $n\mathbb{Z}$ is a commutative ring without unity under the usual addition and multiplication of integers if $n \neq \pm 1$.

3. $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ are commutative rings with unity under the usual addition and multiplication; furthermore, every nonzero element is a unit.

4. $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ is a ring under addition and multiplication modulo n, that is,

$$\begin{aligned} a + b &= \text{remainder on dividing } a+b \text{ by } n \\ a \cdot b &= \text{remainder on dividing } ab \text{ by } n \end{aligned}$$

   $k \in \mathbb{Z}_n$ is a unit if and only if k is relatively prime to n.

5. If R and S are rings, then the direct sum

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

   of R and S is a ring with respect to the binary operations

$$\begin{aligned} (r_1, s_1) + (r_2, s_2) &= (r_1 + r_2, s_1 + s_2), \\ (r_1, s_1) \cdot (r_2, s_2) &= (r_1 \cdot r_2, s_1 \cdot s_2). \end{aligned}$$

6. If R is a ring and X is a nonempty set, then the function ring
$$R^X = \{f \mid f : X \to R\}$$
is a ring with respect to pointwise addition and multiplication, that is,
$$\begin{aligned}(f+g)(x) &= f(x)+g(x),\\ (f\cdot g)(x) &= f(x)\cdot g(x).\end{aligned}$$

7. The collection $M_n(\mathbb{R})$ of $n \times n$ matrices over $\mathbb{R}$ is a ring with respect to the usual addition and multiplication of matrices. ($M_n(\mathbb{R})$ is not a ring with respect to the usual addition and 'multiplication' given by $A * B = AB - BA$ unless $n = 1$.)

8. The polynomial ring $R[x]$ over a ring R; see section 2.

Theorem 1.5 If R is a ring with additive identity 0, then for any $a, b, c \in R$ we have

1. $0a = a0 = 0$;
2. $a(-b) = (-a)b = -(ab)$;
3. $(-a)(-b) = ab$;
4. $a(b-c) = ab - ac$ and $(b-c)a = ba - ca$.

If R is a ring with unity, then this unity 1 is the only multiplicative identity. If $a \in R$ has a multiplicative inverse, then it is unique. Furthermore,

5. $(-1)a = -a$;
6. $(-1)(-1) = 1$.

Definition 1.6 A **subring** of a ring R is a subset S of R that is a ring under induced operations of R.

Theorem 1.7 **(Subring Test)** A nonempty subset S of a ring R is a subring if and only if S is closed under subtraction and multiplication, that is, if $a - b$ and ab are in S whenever a and b are in S.

Example 1.8

1. $\mathbb{N}$ is not a subring of $\mathbb{Z}$;
2. $n\mathbb{Z}$ is a subring of $\mathbb{Z}$;
3. $\{f \in \mathbb{Z}^{\mathbb{Z}} \mid f(0) = 0\}$ is a subring of $\mathbb{Z}^{\mathbb{Z}}$;
4. $\left\{ \begin{bmatrix} a & -b \\ b & a \end{bmatrix} \;\middle|\; a, b \in R \right\}$ is a subring of $M_2(R)$.

Definition 1.9 A nonzero element a in a commutative ring R is called a **zero-divisor** (or **divisor of 0**) if there is a nonzero element b in R such that $ab = 0$.

An **integral domain** is a commutative ring with unity that has no zero-divisors.

Example 1.10

1. In the ring $\mathbb{Z}_n$, the divisors of 0 are precisely those non-zero elements that are not relatively prime to n.
2. The smallest subring of $\mathbb{C}$ that contains $\mathbb{Z}$ and i,
$$\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\},$$
is an integral domain.

Theorem 1.11 Let a, b and c in a commutative ring such that $ab = ac$. If $a \neq 0$ is not a zero-divisor, then $b = c$.

Definition 1.12 A commutative ring with unity is called a **field** if every nonzero element is a unit.

Example 1.13

1. $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ are fields;
2. $\mathbb{Z}$ is an integral domain but not a field;
3. $\mathbb{Z}_n$ is field if and only if n is a prime;
4. $\mathbb{Q}[i] = \{x + yi \mid x, y \in \mathbb{Q}\}$ is a field.

Theorem 1.14 Every field is an integral domain.

Theorem 1.15 In a finite commutative ring with unity every nonzero non-zero-divisor is a unit.

A finite integral domain is a field.

Theorem 1.16 (Wedderburn) A finite ring with unity that has no zero-divisors is a field.

Definition 1.17 The **characteristic** of a ring R is the least positive integer n such that $na = 0$ for all $a \in R$. If no such integer exists, we say that R has characteristic 0. The characteristic of R is denoted by char(R).

Example 1.18 char$(\mathbb{Z}_4 \oplus \mathbb{Z}_6) = 12$

Theorem 1.19 Let R be a ring with unity 1. If 1 has infinite order under addition, then the characteristic of R is 0. If 1 has order n under addition, then the characteristic of R is n.

The characteristic of an integral domain is 0 or prime.

2 Polynomial rings

The integers $\mathbb{Z}$ and polynomial rings $F[x]$ over fields F share many properties.

For example, both have no zero-divisors. There is division of integers with remainder, and one similarly has a division algorithm for polynomials. Furthermore, both allow factorizations into ‘elementary’ elements.

Definition 2.1 If

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

is a polynomial over a ring R where $a_n \neq 0$, we say that n is the **degree of** $f(x)$ or $f(x)$ **has degree** n. The degree of $f(x)$ is denoted by deg $f(x)$.

The term a_n is called the **leading coefficient** of $f(x)$.

If the leading coefficient is the multiplicative identity element of R, we say that $f(x)$ is a **monic polynomial**.

The zero polynomial $f(x) \equiv 0$ has no degree. A polynomial of the form $f(x) = a_0$ is called **constant**. **Linear, quadratic** or **cubic** polynomials are polynomials of degree 1, 2 or 3 respectively.

Theorem 2.2 If D is an integral domain, then $D[x]$ is an integral domain.

Theorem 2.3 (Division Algorithm)

Let F be a field and let $f(x)$ and $g(x) \in F[x]$ with $g(x) \neq 0$. Then there exist unique polynomials $q(x)$ and $r(x)$ in $F[x]$ such that

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

and either $r(x) = 0$ or deg $r(x) <$ deg $g(x)$.

The polynomials $q(x)$ and $r(x)$ are called the **quotient** and **remainder** in the division of $f(x)$ by $g(x)$.

Example 2.4 In $\mathbb{Z}_5[x]$ one has
$x^5+3x^3+x^2+2x+2 = (2x^2+x+3)(3x^3+x^2+4x+2)+3x+1.$

Definition 2.5 Let R be a ring.
If $f(x), g(x) \in R[x]$ we say that $g(x)$ **divides** $f(x)$ **in** $R[x]$ (and write $g(x) \mid f(x)$) or that $g(x)$ **is a factor of** $f(x)$ if there exists an $h(x) \in R[x]$ such that $f(x) = g(x)h(x)$.

An element $a \in R$ is a **zero** (or a **root**) of the polynomial $f(x) \in R[x]$ if $f(a) = 0$.

Corollary 2.6 Let F be a field, $f(x) \in F[x]$ and $a \in F$. Then $f(a)$ is the remainder in the division of $f(x)$ by $x - a$ and a is a zero of $f(x)$ if and only if $x - a$ is a factor of $f(x)$.

Example 2.7 Evaluating the polynomial function for the polynomial

$$f(x) = x^5 + x^2 + 2x + 2$$

in $\mathbb{Z}_3[x]$ yields

r	0	1	2
f(r)	2	0	0

so 2 and 1 are zeros of $f(x)$ and
$f(x) = (x^2 + x + 2)(x - 1)^2(x - 2)$ in $\mathbb{Z}_3[x]$.

Definition 2.8 When F is a field, $f(x) \in F[x]$ and $a \in F$, we say that a is a **zero of multiplicity** k ($k \geq 1$) if $(x-a)^k$ is a factor of $f(x)$ but $(x - a)^{k+1}$ is not a factor of $f(x)$.

Example 2.9 The polynomial

$$f(x) = x^5 + x^2 + 2x + 2 \in \mathbb{Z}_3[x]$$

has zeros 1 and 2. From

$$f(x) = (x^2 + x + 2)(x - 1)^2(x - 2)$$

in $\mathbb{Z}_3[x]$ one sees that 2 and 1 have multiplicities 1 (simple root) and 2 (double root), respectively.

This polynomial has degree 5 and 3 zeros over $\mathbb{Z}_3$, counting multiplicity.

Corollary 2.10 A polynomial of degree n over a field has at most n zeros counting multiplicity.

Definition 2.11 Let D be an integral domain. A polynomial $f(x)$ from $D[x]$ that is neither the zero polynomial nor a unit in $D[x]$ is said to be **irreducible over** D if, whenever $f(x)$ is expressed as a product $f(x) = g(x)h(x)$, with polynomials $g(x)$ and $h(x)$ from $D[x]$, then $g(x)$ or $h(x)$ is a unit in $D[x]$.

A nonzero, nonunit element of $D[x]$ that is not irreducible over D is called **reducible over** D.

Example 2.12 Let $f(x) = 3x^2 - 6$. Then $f(x)$ is

- reducible over $\mathbb{R}$ ($f(x) = 3(x - \sqrt{2})(x + \sqrt{2})$),
- irreducible over $\mathbb{Q}$,
- reducible over $\mathbb{Z}$ ($f(x) = 3 \cdot (x^2 - 2)$),
- irreducible over $\mathbb{Z}_5$ (2 is not a square in $\mathbb{Z}_5$), and
- reducible over $\mathbb{Z}_7$ ($f(x) = 3(x - 3)(x - 4)$).

Theorem 2.13 (Reducibility Test for Degrees 2 and 3)

Let F be a field. If $f(x) \in F[x]$ is of degree 2 or 3, then $f(x)$ is reducible over F if and only if $f(x)$ has a zero in F.

Example 2.14

1. x^2+x+1 is the only irreducible quadratic polynomial over $\mathbb{Z}_2$.
2. x^3+x^2+x+3 is irreducible over $\mathbb{Z}_5$. Evaluating the associated polynomial function over $\mathbb{Z}_5$ yields

r	0	1	2	3	4
r^3+r^2+r+3	3	1	2	2	2

3 Homomorphisms of rings

The rings

$$\begin{aligned} R &= \mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\} \\ S &= \left\{ \begin{bmatrix} x & 2y \\ y & x \end{bmatrix} \;\middle|\; x, y \in \mathbb{Z} \right\} \end{aligned}$$

are defined in very different ways. However, they share many properties. In fact,

$$\begin{bmatrix} x & 2y \\ y & x \end{bmatrix} = xI + yA \quad \text{where } I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \text{ and } A = \begin{bmatrix} 0 & 2 \\ 1 & 0 \end{bmatrix}.$$

Moreover, $A^2 = 2I$, i.e., A represents a square root of 2. Identify $\begin{bmatrix} x & 2y \\ y & x \end{bmatrix} \in S$ with $x + y\sqrt{2} \in R$ and the two rings become algebraically the ‘same’.

Definition 3.1 A **ring homomorphism** φ from a ring R to a ring S is a mapping $\varphi : R \to S$ that preserves the two ring operations; that is, for all $a, b \in R$,

$$\begin{aligned} \varphi(a+b) &= \varphi(a)+\varphi(b) \quad (\varphi \text{ is additive}) \quad \text{and} \\ \varphi(ab) &= \varphi(a)\varphi(b) \qquad\quad (\varphi \text{ is multiplicative}). \end{aligned}$$

A ring homomorphism that is both one-to-one and onto is called a **ring isomorphism**. The rings R and S are then called **isomorphic**.

If $0'$ is the zero-element of S, then

$$\varphi^{-1}(\{0'\}) = \{r \in R \mid \varphi(r) = 0'\}$$

is the **kernel** of φ, denoted by Ker(φ).

Example 3.2

1. For any positive integer m, the mapping $\sigma_m : \mathbb{Z} \to \mathbb{Z}_m$ given by $x \mapsto x \mod m$ is a ring homomorphism with Ker(σ_m) $= m\mathbb{Z}$. This kind of map is behind in the well known test for divisibility by 3 and 9. An integer n with decimal representation $d_k d_{k-1} \ldots d_1 d_0$ is divisible by 3 or 9 if and only if $d_k + d_{k-1} + \ldots + d_1 + d_0$ is divisible by 3 and 9, respectively.
2. The map $\mathbb{Z} \to 3\mathbb{Z}$ given by $z \mapsto 3z$ is not a ring homomorphism. It is additive but not multiplicative.
3. Let R be a commutative ring and let $r \in R$. Then $\varphi : R[x] \to R$ given by $\varphi(f(x)) = f(r)$ is a ring homomorphism (**evaluation homomorphism**).

4. The map $\mathbb{Z}[\sqrt{2}] \to S = \left\{ \begin{bmatrix} x & 2y \\ y & x \end{bmatrix} \;\middle|\; x, y \in \mathbb{Z} \right\}$ given by

$$a + b\sqrt{2} \mapsto \begin{bmatrix} a & 2b \\ b & a \end{bmatrix}$$

is a ring isomorphism.

5. The projection $R \oplus S \to R$ given by $(x, y) \mapsto x$ is a ring homomorphism. Its kernel is isomorphic to S.

6. The map $\varphi : \mathbb{Z}_6 \oplus \mathbb{Z}_6 \to \mathbb{Z}_6$ given by

$$\varphi(x, y) = 3x + 4y$$

is a ring homomorphism. Its kernel is $2\mathbb{Z}_6 \oplus 3\mathbb{Z}_6$.

Theorem 3.3 Let φ be a homomorphism from a ring R into a ring S. Let A be a subring of R and B a subring of S.

1. If 0 is the additive identity in R, then $\varphi(0) = 0'$ is the additive identity in S. If $a \in R$, then $\varphi(-a) = -\varphi(a)$.
2. For any $r \in R$ and any positive integer n, $\varphi(nr) = n\varphi(r)$ and $\varphi(r^n) = (\varphi(r))^n$.
3. $\varphi(A) = \{\varphi(a) \mid a \in A\}$ is a subring of S.
4. $\varphi^{-1}(B) = \{r \in R \mid \varphi(r) \in B\}$ is a subring of R.
5. If R is commutative, then $\varphi(R)$ is commutative.
6. If R has unity 1 and $\varphi(1) \neq 0'$, then $\varphi(1)$ is a unity for $\varphi(R)$.
7. φ is an isomorphism if and only if φ is onto and $\mathrm{Ker}(\varphi) = \{0\}$. In this case, φ^{-1} is an isomorphism from S onto R.

Example 3.4

1. $\varphi : \mathbb{Z}_2 \to \mathbb{Z}_6 : z \mapsto 3z$ is a ring homomorphism that is not onto. $\varphi(1) = 3$ is a unity of $\varphi(\mathbb{Z}_2)$ but not of $\mathbb{Z}_6$.
2. $\mathbb{Z}$ admits precisely two ring homomorphisms to itself, the identity and the trivial homomorphism that takes every integer to 0.
3. $\mathbb{Z}_6$ admits precisely four ring homomorphisms to itself.
4. There are precisely nine ring homomorphisms from $\mathbb{Z}_6 \oplus \mathbb{Z}_6$ to $\mathbb{Z}_6$.
5. The rings $\mathbb{Z}_5$ and $2\mathbb{Z}_{10}$ are isomorphic.

Remark 3.5 Isomorphic rings have the same algebraic properties (number of elements, characteristic, being commutative, having a unity, number of units, being a field, number of zero-divisors, being an integral domain, number of solutions of certain algebraic equations, etc.). If a ring has an algebraic property that another rings does not have, then the two rings cannot be isomorphic.
For example, $\mathbb{Z}_6 \oplus \mathbb{Z}_6$ and $\mathbb{Z}_{36}$ are not isomorphic, because $\mathbb{Z}_6 \oplus \mathbb{Z}_6$ has characteristic 6 whereas $\mathbb{Z}_{36}$ has characteristic 36.

Theorem 3.6 Let $\varphi : R \to S$ be a ring homomorphism, $H = \text{Ker}(\varphi)$ and $a \in R$. Then

$$\varphi^{-1}\{\varphi(a)\} = a + H = \{a + x \mid x \in H\}.$$

Example 3.7

1. Let $\varphi : \mathbb{Z} \to \mathbb{Z}_m : x \mapsto x \mod m$. Then
$$\begin{aligned}\varphi^{-1}\{\varphi(a)\} &= \{z \in \mathbb{Z} \mid \text{ has the same remainder as } a \\ &\qquad \text{on division by } m\} \\ &= a + m\mathbb{Z}.\end{aligned}$$

2. Let $\varphi : \mathbb{Z}[x] \to \mathbb{Z} : f(x) \mapsto f(0)$. Then
$$\begin{aligned}\varphi^{-1}\{\varphi(f(x))\} &= \{g(x) \in \mathbb{Z}[x] \mid \ g(x) \text{ has the same} \\ &\qquad \text{value as } f(x) \text{ at } 0\} \\ &= f(x) + x\mathbb{Z}[x].\end{aligned}$$

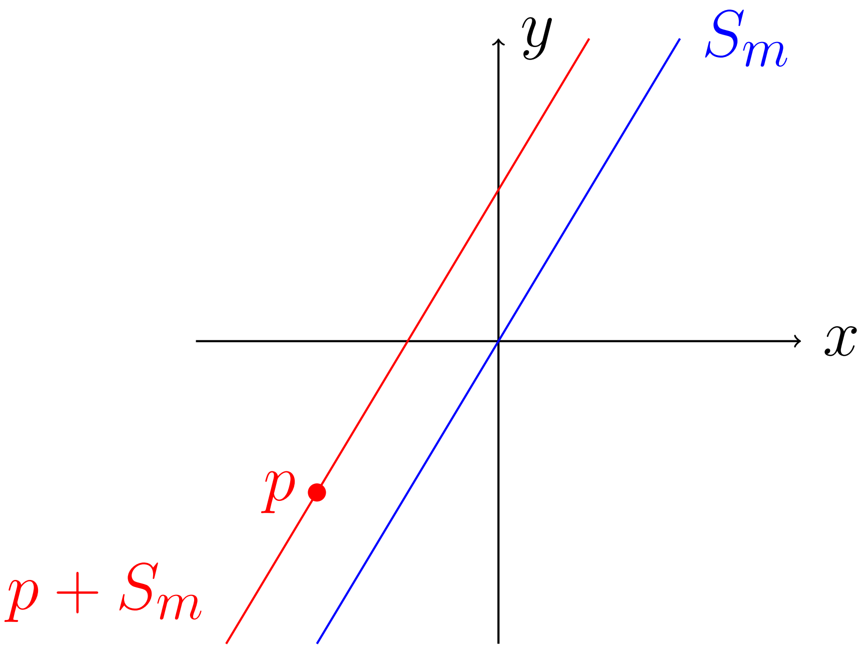
Definition 3.8 Let S be a subring of a ring R. A coset of S in R is a set of the form

$$u + S = \{u + s \mid s \in S\}$$

for $u \in R$.

Example 3.9 $\mathbb{R}^2$ becomes a ring R with respect to usual addition and the multiplication $(x_1, y_1) \cdot (x_2, y_2) = (0, 0)$.

$S = \{(x, mx) \mid x \in \mathbb{R}\}$ is a subring of R (represented by a line L of slope m through the origin). A coset of S is represented by a line parallel to L.



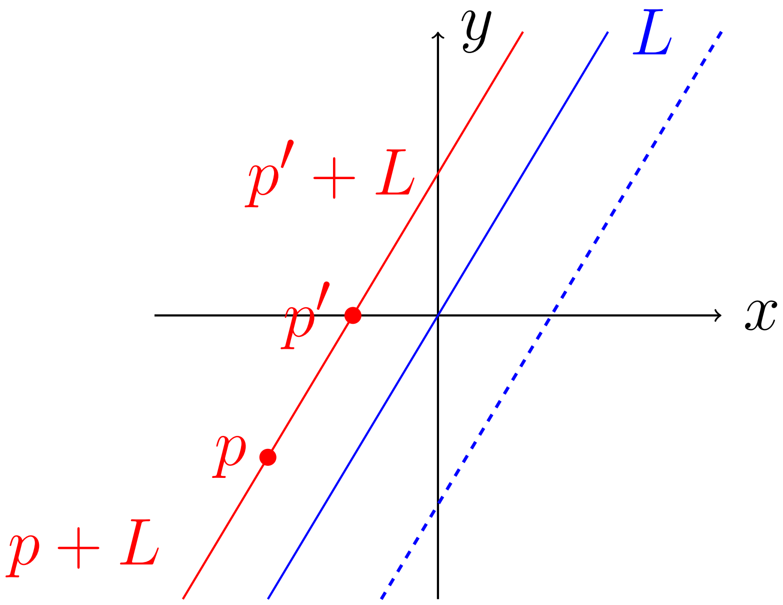
Theorem 3.10 Let S be a subring of a ring R. Then

$$u + S = v + S \text{ if and only if } v - u \in S.$$

Every element of R belongs to exactly one coset of S.

Example 3.11 In Example 3.9 of $\mathbb{R}^2$ as a ring with usual vector addition and trivial multiplication a line ($=$ coset of a suitable subring S) can be descibed by any point on the line and a direction vector ($=$ non-zero element of S).

All lines parallel to a line L through the origin partition $\mathbb{R}^2$.



Theorem 3.12 Let R be a ring with unity e. The mapping $\varphi : \mathbb{Z} \to R$ given by $\varphi(n) = ne$ is a ring homomorphism.

Corollary 3.13 If R is a ring with unity and the characteristic of R is $n > 0$, then R contains a subring isomorphic to $\mathbb{Z}_n$. If the characteristic of R is 0, then R contains a subring isomorphic to $\mathbb{Z}$.

Corollary 3.14 (Steinitz, 1910)
If F is a field of characteristic p, then F contains a subfield isomorphic to $\mathbb{Z}_p$. If F is a field of characteristic 0, then F contains a subfield isomorphic to the rational numbers $\mathbb{Q}$.

Example 3.15 $\mathbb{Z}_3[i] = \{a + bi \mid a, b \in \mathbb{Z}_3\}$ with addition

$$(a + bi) + (c + di) = (a + c) + (b + d)i$$

and multiplication

$$(a + bi)(c + di) = (ac - bd) + (ad + bc)i$$

is a field with 9 elements. F has characteristic 3 and $\{0, 1, 2\}$ is a subfield of F isomorphic to $\mathbb{Z}_3$.

4 Factorization of polynomials

$\mathbb{Z}$ and $F[x]$ where F is a field are both integral domains and have a division algorithm. Both have 'indecomposable' elements.

Are there further similarities between these two rings?

E.g, is there a 'prime factorization' in $F[x]$ and if so, is it unique?

Theorem 4.1 Let $f(x) \in \mathbb{Z}[x]$. If $f(x)$ is reducible over $\mathbb{Q}$, then it is reducible over $\mathbb{Z}$. More precisely, $f(x)$ factors into a product of two polynomials of lower degrees r and s in $\mathbb{Q}[x]$ if and only if it has such a factorization with polynomials of the same degrees r and s in $\mathbb{Z}[x]$.

Example 4.2

1. The quadratic polynomial

   $$6x^2 + 7x - 3 \in \mathbb{Z}[x]$$

   has the factorization

   $$\left(3x + \frac{9}{2}\right)\left(2x - \frac{2}{3}\right)$$

   over $\mathbb{Q}$.

One then obtains

$$\begin{aligned}\left(3x+\frac{9}{2}\right)\left(2x-\frac{2}{3}\right) &= \frac{1}{2}(6x+9)\cdot\frac{1}{3}(6x-2)\\ &\quad \text{(clear denominators)}\\ &= \frac{3}{2}(2x+3)\cdot\frac{2}{3}(3x-1)\\ &\quad \text{(clear gcd's of coefficients)}\\ &= (2x+3)(3x-1)\end{aligned}$$

2. x^4+x^2+2 is irreducible over $\mathbb{Q}$.

Theorem 4.3 Let $\sigma_m : \mathbb{Z} \to \mathbb{Z}_m$ be the natural homomorphism given by

$$\begin{aligned}\sigma_m(a) = a \pmod{m} \\ = \text{ the remainder of } a \text{ upon division by } m\end{aligned}$$

for $a \in \mathbb{Z}$. Then $\tilde{\sigma}_m : \mathbb{Z}[x] \to \mathbb{Z}_m[x]$ defined by

$$\tilde{\sigma}_m(a_n x^n + \ldots + a_1 x + a_0) = \sigma_m(a_n)x^n + \ldots + \sigma_m(a_1)x + \sigma_m(a_0)$$

is a homomorphism from $\mathbb{Z}[x]$ onto $\mathbb{Z}_m[x]$.
($\tilde{\sigma}_m$ reduces all the coefficients of $f(x) \in \mathbb{Z}[x]$ modulo m. This may reduce the degree of the polynomial.)

Example 4.4 When $f(x) = 6x^3 - 4x^2 + x + 8 \in \mathbb{Z}[x]$ one obtains

$$\begin{aligned}\tilde{\sigma}_3(f(x)) &= 2x^2 + x + 2 \in \mathbb{Z}_3[x] \quad \text{and} \\ \tilde{\sigma}_5(f(x)) &= x^3 + x^2 + x + 3 \in \mathbb{Z}_5[x].\end{aligned}$$

Theorem 4.5 (Mod p Irreducibility Test)

Let p be a prime and suppose that $f(x) \in \mathbb{Z}[x]$ with deg $f(x) \geq 1$. Let $\bar{f}(x)$ be the polynomial in $\mathbb{Z}_p[x]$ obtained from $f(x)$ by reducing all the coefficients of $f(x)$ modulo p. If $\bar{f}(x)$ is irreducible over $\mathbb{Z}_p$ and deg $\bar{f}(x) =$ deg $f(x)$, then $f(x)$ is irreducible over $\mathbb{Q}$.

Example 4.6

1. When $f(x) = 6x^3 - 4x^2 + x + 8 \in \mathbb{Z}[x]$ one has
$$f_5(x) = \tilde{\sigma}_5(f(x)) = x^3 + x^2 + x + 3.$$
Since $f_5(x)$ is irreducible over $\mathbb{Z}_5$ by 2.14.2, $f(x)$ is irreducible over $\mathbb{Q}$.

2. When $g(x) = 5x^4 + 2x^3 - 3x^2 + 4x + 9 \in \mathbb{Z}[x]$ one finds

$$\begin{aligned} g_2(x) &= \tilde{\sigma}_2(g(x)) = x^4 + x^2 + 1 \\ &= (x^2 + x + 1)^2 \text{ and} \\ g_3(x) &= \tilde{\sigma}_3(g(x)) = 2x^4 + 2x^3 + x \\ &= 2x(x^3 + x^2 + 2). \end{aligned}$$

   Since the factorizations don't match, $g(x)$ must be irreducible over $\mathbb{Q}$.

3. When $h(x) = 2x^3 + 4x^2 + x + 2 \in \mathbb{Z}[x]$ one finds

$$h_2(x) = \tilde{\sigma}_2(h(x)) = x.$$

   Although $h_2(x)$ is irreducible over $\mathbb{Z}_2$, $h(x)$ is not irreducible over $\mathbb{Q}$. In fact, $h(x) = (x + 2)(2x^2 + 1)$.

Theorem 4.7 (Eisenstein's Criterion, 1850)
Let $f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_0 \in \mathbb{Z}[x]$. If there is a prime p such that

$$p \nmid a_n, p \mid a_{n-1}, \ldots, p \mid a_0 \text{ and } p^2 \nmid a_0,$$

then $f(x)$ is irreducible over $\mathbb{Q}$.

Example 4.8

1. $2x^5 + 6x^3 - 9x^2 + 18x - 6$ satisfies the assumptions of Eisenstein's criterion for $p = 3$ and thus is irreducible over $\mathbb{Q}$.
2. $f(x) = 2x^3 - 10x^2 - 20x + 10$ satisfies the assumptions of Eisenstein's criterion for $p = 5$. Thus $f(x)$ is irreducible over $\mathbb{Q}$. However, $f(x)$ is not irreducible over $\mathbb{Z}$ because $f(x) = 2(x^3 - 5x^2 - 10x + 5)$.

3. Eisenstein's criterion does apply neither to

$$x^2 + 2x + 4 \quad \text{nor to} \quad x^2 + 4x + 4.$$

(The only possible prime to check is $p = 2$.)

Indeed, the first polynomial is irreducible over $\mathbb{Q}$ (because $x^2 + 2x + 4 = (x + 1)^2 + 3$ has no zeros) whereas the second polynomial is reducible over $\mathbb{Q}$ (with factorization $x^2 + 4x + 4 = (x + 2)^2$).

Theorem 4.9 Every polynomial in $\mathbb{Z}[x]$ that is not the zero polynomial or a unit in $\mathbb{Z}[x]$ can be written in the form

$$b_1b_2\cdots b_sp_1(x)p_2(x)\cdots p_m(x)$$

where the b_j's are primes in $\mathbb{Z}$, and the $p_i(x)$'s are irreducible polynomials of positive degree. Furthermore, if

$$b_1b_2\cdots b_sp_1(x)p_2(x)\cdots p_m(x) = c_1c_2\cdots c_tq_1(x)q_2(x)\cdots q_n(x)$$

where the b_k's and c_l's are primes in $\mathbb{Z}$, and the $p_i(x)$'s and $q_j(x)$'s are irreducible polynomials over $\mathbb{Z}$ of positive degree, then $s = t$, $m = n$, and, after renumbering the c_k's and $q_j(x)$'s, we have $b_i = \pm c_i$ for $i = 1, \ldots, s$; and $p_i(x) = \pm q_i(x)$ for $i = 1, \ldots, m$.

Theorem 4.10 Let F be a field. Then $F[x]$ is a unique factorization domain, that is, every polynomial in $F[x]$ that is neither the zero polynomial nor a unit in $F[x]$ can be written in the form

$$p_1(x)p_2(x)\cdots p_m(x)$$

where the $p_i(x)$'s are irreducible polynomials over F of positive degree. Furthermore, if

$$p_1(x)p_2(x)\cdots p_m(x) = q_1(x)q_2(x)\cdots q_n(x)$$

where the $p_i(x)$'s and $q_j(x)$'s are irreducible polynomials over F of positive degree, then $m = n$, and, after renumbering the $q_j(x)$'s, we have $p_i(x) = c_i q_i(x)$ for $i = 1, \ldots, m$ and some $c_i \in F$, $c_i \neq 0$.

Remark 4.11 The notion of irreducible polynomials and factorizations can be generalized to integral domains D. A nonzero element p that is not a unit of D is an **irreducible of** D if in any factorization $p = ab$ in D either a or b is a unit.
An integral domain D is a **unique factorization domain** if the following conditions are satisfied:

- Every element of D that is neither 0 nor a unit can be factored into a product of a finite number of irreducibles.
- If $p_1 \cdots p_r$ and $q_1 \cdots q_s$ are two factorizations of the same element of D into irreducibles, then $r = s$ and the q_j can be renumbered so that $q_i = u_i p_i$ for some unit u_i in D.

It is an important question which integral domains are unique factorization domains.

A number of results in number theory follow from the fact that certain subrings of $\mathbb{C}$ are unique factorization domains. For example, $\mathbb{Z}[i]$ is a unique factorization domain and can be used to determine which natural numbers can be written as a sum of two squares.

Another example of a unique factorization domain is the ring $\mathbb{Z}[\omega] \leq \mathbb{C}$ where $\omega = \frac{1}{2}(-1+\sqrt{-3})$. A non-zero solution to Fermat's last theorem for $n = 3$, that is, $x^3 + y^3 = z^3$ where x, y, z are positive integers, yields factorizations

$$(x+y)(x+y\omega)(x+y\omega^2) = z^3$$

in $\mathbb{Z}[\omega]$. An analysis of irreducibles and of such factorizations in $\mathbb{Z}[\omega]$ leads to a contradiction.

5 Ideals and factor rings

Addition and multiplication in $\mathbb{Z}_2$ reflect how even or odd integers are added or multiplied. One can therefore obtain $\mathbb{Z}_2$ as a ring from $\mathbb{Z}$ by considering the subring of all even integers as one new object and the collection of all odd integers as another new object.

Is there a general principle behind this method that applies to arbitrary rings and subrings and other collections of elements?

Definition 5.1 (see 3.8) Let S be a subring of a ring R. A coset of S in R is a set of the form

$$u + S = \{u + s \mid s \in S\}$$

for $u \in R$.

Theorem 5.2 (see 3.10)

Let S be a subring of a ring R. Then

$$u + S = v + S \text{ if and only if } v - u \in S.$$

Every element of R belongs to exactly one coset of S.

Theorem 5.3 Let S be a subring of a ring R.

1. Addition of cosets of S is well defined by the equation
$$(u+S)+(v+S)=(u+v)+S$$
2. Multiplication of cosets of S is well defined by the equation
$$(u+S)(v+S)=(uv)+S$$
if and only if $us \in S$ and $sv \in S$ for all $s \in S$.

Definition 5.4 A subring A of a ring R is called a (two-sided) **ideal** of R if A for every $r \in R$ and every $a \in A$ both ra and ar are in A ('absorbing property' of an ideal).

Example 5.5

1. Every ring R has two ideals, the **improper ideal** R and the **trivial ideal** $\{0\}$. A **proper nontrivial ideal** of R is an ideal A of R such that $A \neq R$ and $A \neq \{0\}$.
2. Every ideal of $\mathbb{Z}$ is of the form $n\mathbb{Z}$ for some nonnegative integer n.

   Addition and multiplication of cosets of $n\mathbb{Z}$ reflect how elements in $\mathbb{Z}_n$ are added or multiplied.
3. $\mathbb{Z}$ is a subring of $\mathbb{Q}$ but not an ideal of $\mathbb{Q}$.
4. The kernel of a ring homomorphism from a ring R to a ring S is an ideal of R.

5. If R is a commutative ring with unity and $a \in R$, then the set
$$\langle a \rangle = Ra = \{ra \mid r \in R\}$$
of all multiples of a is an ideal, called the **principal ideal generated by** a. An ideal I of R is a **principal ideal** if $I = \langle a \rangle$ for some $a \in R$.

6. The cosets of $A = \langle 3 + i \rangle$ in $\mathbb{Z}[i]$ are precisely the sets $k + A$ where $k = 0, 1, \ldots, 9$. Two such cosets are added and multiplied according to the rule
$$\begin{aligned}(k + A) + (m + A) &= (k + m)_{(\mathrm{mod}\,10)} + A,\\ (k + A) \cdot (m + A) &= (km)_{(\mathrm{mod}\,10)} + A.\end{aligned}$$

Theorem 5.6 (Ideal test)

A nonempty subset A of a ring R is an ideal of R if

1. $a - b \in A$ whenever $a, b \in A$;
2. ra and ar are in A whenever $a \in A$ and $r \in R$.

Example 5.7

1. The set
$$\{f \in \mathbb{Q}^{\mathbb{Z}} \mid f(0) = 0\}$$
is an ideal of $\mathbb{Q}^{\mathbb{Z}}$.
2. The set
$$\{f(x) \in \mathbb{Z}[x] \mid f(0) \text{ is even}\}$$
is an ideal of $\mathbb{Z}[x]$.

Definition 5.8 A **principal ideal domain** is an integral domain in which every ideal is a principal ideal.

Example 5.9

1. $\mathbb{Z}$ is a principal ideal domain.
2. $\mathbb{Z}[x]$ is not a principal ideal domain.

$$A = \{f(x) \in \mathbb{Z}[x] \mid f(0) \text{ is even}\}$$

is an ideal but not a principal ideal.

Theorem 5.10 Let F be a field. Then $F[x]$ is a principal ideal domain. Moreover, if I a nonzero ideal in $F[x]$, and $g(x)$ an element of $F[x]$, then $I = \langle g(x) \rangle$ if and only if $g(x)$ is a nonzero polynomial of minimum degree in I.

Example 5.11 $A = \{f(x) \in \mathbb{R}[x] \mid f(i) = 0\}$ is an ideal of $\mathbb{R}[x]$ and $A = \langle x^2 + 1 \rangle$.

Theorem 5.12 A commutative ring with unity is a field if and only if it has no proper nontrivial ideals.

Theorem 5.13 Let A be a subring of a ring R. The set of cosets $\{r + A \mid r \in R\}$ is a ring under the operations

$$\begin{aligned} (s + A) + (t + A) &= (s + t) + A \\ (s + A)(t + A) &= (st) + A \end{aligned}$$

if and only if A is an ideal of R.

The ring R/A of cosets of the ideal A is the **factor ring** or **quotient ring** of R modulo A.

Example 5.14

1. $\mathbb{Z}/\langle n\rangle$ is isomorphic to $\mathbb{Z}_n$.
2. $\mathbb{Z}[i]/\langle 3+i\rangle$ is isomorphic to $\mathbb{Z}_{10}$.
3. $\{0\}\oplus R_2$ is an ideal of $R_1\oplus R_2$ and $(R_1\oplus R_2)/(\{0\}\oplus R_2)$ is isomorphic to R_1.
4. $\mathbb{R}[x]/\langle x^2+1\rangle$ is isomorphic to $\mathbb{C}$.

Theorem 5.15 (First Isomorphism Theorem for Rings)

Let φ be a ring homomorphism from R to S. Then the mapping from $R/\mathrm{Ker}(\varphi)$ to $\varphi(R)$, given by

$$r+\mathrm{Ker}(\varphi)\mapsto\varphi(r)$$

is an isomorphism. In symbols, $R/\mathrm{Ker}(\varphi)\cong\varphi(R)$.

Example 5.16

1. $\mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}_m$
2. $(R_1 \oplus R_2)/(\{0\} \oplus R_2) \cong R_1$.
3. $R[x]/\langle x \rangle \cong R$
4. $\mathbb{R}[x]/\langle x^2 + 1 \rangle \cong \mathbb{C}$.

Theorem 5.17 Let φ be a homomorphism from a ring R into a ring S. Let A be an ideal of R and B an ideal of S.

1. If φ is onto S, then $\varphi(A)$ is an ideal.
2. $\varphi^{-1}(B) = \{r \in R \mid \varphi(r) \in B\}$ is an ideal of R.

Example 5.18 The inclusion $\varphi : \mathbb{Z} \to \mathbb{Q} : z \mapsto z$ is a ring homomorphism that is not onto. $\mathbb{Z}$ is an ideal of $\mathbb{Z}$, but $\varphi(\mathbb{Z})$ is not an ideal of $\mathbb{Q}$.

Definition 5.19 A proper ideal A of R is said to be a **maximal ideal** of R if there is no proper ideal of R properly containing A, that is, whenever B is an ideal of R such that $A \subseteq B \subseteq R$, then either $B = A$ or $B = R$.

Example 5.20 An ideal $n\mathbb{Z}$ of $\mathbb{Z}$ where n is a positive integer is a maximal ideal if and only if n is prime.

Theorem 5.21 Let R be a commutative ring with unity and let A be a proper ideal of R. Then R/A is a field if and only if A is a maximal ideal of R.

Example 5.22

1. $\mathbb{Z}/\langle p\rangle$, p prime, is a field.
2. $\langle x^2+1\rangle$ is a maximal ideal of $\mathbb{R}[x]$.

Theorem 5.23 Let F be a field and let $p(x) \in F[x]$. Then $\langle p(x)\rangle$ is a maximal ideal of $F[x]$ if and only if $p(x)$ is irreducible over F.

Corollary 5.24 Let F be a field and $p(x)$ an irreducible polynomial over F. Then $F[x]/\langle p(x)\rangle$ is a field.

Example 5.25 $\mathbb{Z}_2[x]/\langle x^2+x+1\rangle$ is a field with 4 elements, and $\mathbb{Z}_3[x]/\langle x^2+1\rangle$ is a field with 9 elements.

6 Vector spaces

From Linear Algebra we know that the collection of all polynomials of degree at most 5 with real coefficients plus the zero polynomial form a 6-dimensional (real) vector space with basis $\{1, x, x^2, x^3, x^4, x^5\}$. Similarly, $\mathbb{R}[x]$ is an infinite-dimensional vector space.

What is the general notion of vector space so that it can be applied to, say, $F[x]$ where F is a field?

Does every vector space in this general setting have a basis and a dimension?

Definition 6.1 A set V is said to be a **vector space** over a field F if V is a commutative group under addition (denoted by $+$) and, if for each $a \in F$ and $v \in V$, there is an element av in V such that the following conditions hold for all $a, b \in F$ and all $u, v \in V$.

(V1) $a(u+v) = au + av$,
(V2) $(a+b)v = av + bv$,
(V3) $a(bv) = (ab)v$,
(V4) $1v = v$.

The members of V are called **vectors**; the members of F are called **scalars**. The operation that combines a scalar a and a vector v to form the vector av is called **scalar multiplication**.

A subset U of a vector space V over a field F is a **subspace** of V if U is also a vector space over F under the operations of V.

Example 6.2

1. Let E be a field and $F \subseteq E$ be a subfield of E. Then E is a vector space over F.
2. $F[x]$ is a vector space over the field F.

Theorem 6.3 (Subspace Test)

A nonempty subset U of a vector space V over a field F is a subspace of V if

1. $u - v \in U$ whenever $u, v \in U$;
2. $au \in U$ whenever $a \in F$ and $u \in U$.

Proof.

By the first item and the subgroup criterion from Group Theory (Math240) U is a subgroup of V. The second item ensures that the operation of scalar multiplication on U is defined. The properties V1-V4 now hold on U since they hold on V

Example 6.4 $\mathbb{Q}(\sqrt{2})$ is a vector subspace of $\mathbb{R}$ over $\mathbb{Q}$.

Definition 6.5 Let V be a vector space over a field F and let $v_1, v_2, \ldots, v_n$ be (not necessarily distinct) elements of V. Then any vector of the form

$$a_1v_1 + a_2v_2 + \ldots + a_nv_n$$

for $a_1, a_2, \ldots, a_n \in F$ is called a **linear combination of** $v_1, v_2, \ldots, v_n$.

The subset

$$\begin{aligned} \langle v_1, v_2, \ldots, v_n \rangle = \{ & a_1v_1 + a_2v_2 + \ldots + a_nv_n \\ & \mid a_1, a_2, \ldots, a_n \in F\} \end{aligned}$$

is called the **subspace of** V **spanned by** $v_1, v_2, \ldots, v_n$.

If $\langle v_1, v_2, \ldots, v_n \rangle = V$, we say that $\{v_1, v_2, \ldots, v_n\}$ **spans** V.

Example 6.6 $\langle 1, \sqrt{2} \rangle = \mathbb{Q}(\sqrt{2})$ in $\mathbb{R}$ over $\mathbb{Q}$.

Definition 6.7 Let V be a vector space over a field F. A set of vectors $\{v_1, v_2, \ldots, v_n\}$ is said to be **linearly dependent** over the field F if there are elements $a_1, a_2, \ldots, a_n$ from F, not all zero, such that

$$a_1v_1 + a_2v_2 + \ldots + a_nv_n = 0.$$

A set of vectors that is not linearly dependent over F are called **linearly independent over** F.
A subset B of V is called a **basis** for V if B is linearly independent over F and B spans V.

Example 6.8 $\{1, \sqrt{2}\}$ is a basis for $\mathbb{Q}(\sqrt{2})$ over $\mathbb{Q}$.

Theorem 6.9 Every vector space has a basis.

This theorem is difficult to prove (the usual proof requires Zorn's lemma) and the proof will be omitted.

Theorem 6.10 If $\{u_1, u_2, \ldots, u_m\}$ and $\{w_1, w_2, \ldots, w_n\}$ are both bases of a vector space V, then $m = n$.

Proof.

It uses the following result, known as Steinitz replacement lemma.

If $\{v_1, \ldots, v_m\}$ is a set of m linearly independent vectors in a vector space V, and $W = \{w_1, \ldots, w_n\}$ span V, then:

1. $m \leq n$

2. The set $\{v_1, \ldots, v_m, w_{m+1}, \ldots, w_n\}$ spans V, possibly after reordering the w_i.

Since W spans V we can write $v_1 = \sum a_i w_i$ and since the v_i are linearly independent, $v_1 \neq 0$ so some $a_i \neq 0$. We reorder the w_i so that $a_1 \neq 0$ and we can replace w_1 by v_1, i.e.,

$v_1, w_2, \ldots, w_n$ span V. Indeed,

$$w_1 = (1/a_1)(v_1 - \sum_{i>1} a_i w_i)$$

so any linear combination of the w_i is a linear combination of $v_1, w_2, \ldots, w_n$.

Now $v_2 = b_1 v_1 + \sum_{i>1} b_i w_i$ and we claim that, for some $i > 1, b_i \neq 0$. Indeed, if not $v_2 = b_1 v_1$ contradicting the linearly independence of the v_i. Reorder the w_i so that $b_2 \neq 0$ and repeat the argument. Namely,

$$w_2 = (1/b_2)(v_2 - b_1 v_1 - \sum_{i>2} b_i w_i)$$

so we can replace w_2 by v_2.

Definition 6.11 A vector space that has a basis consisting of n elements is said to have **dimension** n.

The trivial vector space $\{0\}$ is said to be spanned by the empty set and to have dimension 0. A vector space that has a finite basis is called **finite dimensional**; otherwise, it is called **infinite dimensional**.

Example 6.12 $\mathbb{Q}(\sqrt{2})$ is 2-dimensional over $\mathbb{Q}$.
$\mathbb{Q}[x]$ is infinite dimensional over $\mathbb{Q}$.

Remark 6.13 An (n, k) **linear code** over a finite field F is a k-dimensional vector subspace U of an n-dimensional vector space V over F. In case $F = \mathbb{Z}_2$ one speaks of a **binary linear code**. If $\{u_1, \ldots, u_k\}$ is a basis for U and $\{v_1, \ldots, v_n\}$ is a basis for V, then a message word $(c_1, \ldots, c_k) \in F^k$ is encoded as $(d_1, \ldots, d_n) \in F^n$ where $c_1u_1 + \ldots c_ku_k = d_1v_1 + \ldots d_nv_n$. (So the d_i are the coefficients of $u = c_1u_1 + \ldots c_ku_k \in U$ with respect to the basis $\{v_1, \ldots, v_n\}$ for V.) A nice class of codes is obtained as follows. Let

$$V = F[x]/\langle x^n - 1\rangle.$$

V is a vector space over F of dimension n. If $g(x) \in F[x]$ is a divisor of $x^n - 1$, the principal ideal $\langle g(x)\rangle$ generated by $g(x)$ is a vector subspace of $F[x]$ that comprises $\langle x^n - 1\rangle$

and thus gives rise to a vector subspace

$$U = \langle g(x) \rangle / \langle x^n - 1 \rangle$$

of V dimension $n - r$ where r is the degree of $g(x)$. U is a **linear cyclic code**, because $xf(x) \pmod{x^n - 1} \in U$ for each $f(x) \in U$ and the coefficients of $xf(x) \pmod{x^n - 1}$ are obtained from the coefficients of $f(x)$ by a cyclic shift. A message word $f(x)$ (a polynomial of degree less than $n - r$) is encoded as $f(x)g(x)$. In order to check whether a received word is correct divide by $g(x)$. If the remainder is non-zero, an error has occurred in transmission.

7 Extension fields

$\mathbb{R}$ is a subfield of $\mathbb{C}$. In order to get from $\mathbb{R}$ to $\mathbb{C}$ all one needs is the imaginary unit i, $i^2 = -1$. Then apply the algebraic operations to obtain all complex numbers. Also passing from from $\mathbb{R}$ to $\mathbb{C}$ makes the polynomial $x^2 + 1 \in \mathbb{R}[x]$, which is irreducible over $\mathbb{R}$, reducible.

Can we do something similar for any polynomial $f(x) \in F[x]$, that is, is there always a larger field containing the field F such that $f(x)$ has a zero in it. If so, how can such a field be obtained?

Definition 7.1 A field E is an **extension field** of a field F if $F \subseteq E$ and the operations of F are those of E restricted to F. (That is, F is a subfield of E.)

Example 7.2

1. $\mathbb{R}$ and $\mathbb{Q}(\sqrt{2})$ are extension fields of $\mathbb{Q}$.
2. $\mathbb{R}$ and $\mathbb{Q}(\sqrt[4]{2})$ are extension fields of $\mathbb{Q}(\sqrt{2})$.
3. $\mathbb{C}$ is an extension field of $\mathbb{R}$.

Definition 7.3 Let F be a field and let $a_1, a_2, \ldots, a_n$ be elements of some extension field E of F. Then we denote by $F(a_1, a_2, \ldots, a_n)$ the smallest subfield of E that contains F and the set $\{a_1, a_2, \ldots, a_n\}$.

Example 7.4

1. $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$
2. $\mathbb{Q}(\sqrt[4]{2}) = \{a + b\sqrt[4]{2} + c\sqrt{2} + d\sqrt[4]{8} \mid a, b, c, d \in \mathbb{Q}\}$
3. $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \mid a, b, c, d \in \mathbb{Q}\}$

Theorem 7.5 (Fundamental Theorem of Field Theory, Kronecker's Theorem, 1887)

Let F be a field and let $f(x)$ be a non-constant polynomial in $F[x]$. Then there is an extension field E of F in which $f(x)$ has a zero.

Example 7.6 $E = \{a + bw \mid a, b \in \mathbb{Z}_3\}$ is an extension field of $\mathbb{Z}_3$ in which

$$f(x) = x^2 + x + 2 \in \mathbb{Z}_3[x]$$

has a zero. Addition and multiplication in E are given by

$$\begin{aligned}(a + bw) + (c + dw) &= (a + c) + (b + d)w \\ (a + bw)(c + dw) &= (ac + bd) \\ &\quad +(ad + bc + 2bd)w\end{aligned}$$

Definition 7.7 Let E be an extension field of F and let $f(x) \in F[x]$. We say that $f(x)$ **splits** in E if $f(x)$ can be factored as a product of linear factors in $E[x]$. We call E a **splitting field for** $f(x)$ **over** F if $f(x)$ splits in E but in no proper intermediate field between E and F.

Example 7.8

1. $x^2 - 2 \in \mathbb{Q}[x]$ splits in $\mathbb{R}$ but $\mathbb{Q}(\sqrt{2})$ is a splitting field of $x^2 - 2$ over $\mathbb{Q}$.
2. $\mathbb{C}$ is a splitting field for x^2+1 over $\mathbb{R}$, and $\mathbb{Q}(i)$ is a splitting field for $x^2 + 1$ over $\mathbb{Q}$.
3. $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ is a splitting field for
$$x^4 - 5x^2 + 6 = (x^2 - 2)(x^2 - 3)$$
over $\mathbb{Q}$.

Theorem 7.9 Let F be a field and let $f(x)$ be a non-constant element of $F[x]$. Then there exists a splitting field E for $f(x)$ over F.

Example 7.10

1. $\mathbb{Q}(\sqrt[4]{2}, i)$ is a splitting field of $x^4 - 2$ over $\mathbb{Q}$.
2. A splitting field for $x^4 - 5x^2 + 6 = (x^2 - 2)(x^2 - 3)$ over $\mathbb{Q}(\sqrt{6})$ is $\mathbb{Q}(\sqrt{2}, \sqrt{3})$.

Theorem 7.11 Let F be a field and let $p(x) \in F[x]$ be irreducible over F. If a is a zero of $p(x)$ in some extension E of F, then $F(a)$ is isomorphic to $F(a) \cong F[x]/\langle p(x) \rangle$. Furthermore, if deg $p(x) = n$, then every member of $F(a)$ can be uniquely expressed in the form

$$c_{n-1}a^{n-1} + c_{n-2}a^{n-2} + \cdots + c_1 a + c_0,$$

where $c_0, c_1, \ldots, c_{n-1} \in F$, that is, $\{1, a, \ldots, a^{n-1}\}$ is a basis for $F(a)$ over F.

Corollary 7.12 Let F be a field and let $p(x) \in F[x]$ be irreducible over F. If a is a zero of $p(x)$ in some extension E of F and b is a zero of $p(x)$ in some extension E' of F, then the fields $F(a)$ and $F(b)$ are isomorphic.

Example 7.13

1. The fields $\mathbb{Q}\left(\frac{1+i}{\sqrt{2}}\right)$ and $\mathbb{Q}\left(\frac{1-i}{\sqrt{2}}\right)$ are isomorphic. Both complex numbers $\frac{1+i}{\sqrt{2}}$ and $\frac{1-i}{\sqrt{2}}$ are zeros of the irreducible polynomial x^4+1 over $\mathbb{Q}$. Complex conjugation is an isomorphism between the two fields.
2. $\sqrt{2}$ and $\sqrt{3}$ are zeros of the polynomial $x^4-5x^2+6=(x^2-2)(x^2-3)$. However, the fields $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{3})$ are not isomorphic.

Theorem 7.14 Let F be a field and let $f(x) \in F[x]$. Then any two splitting fields for $f(x)$ over F are isomorphic.

Example 7.15 The splitting field of

$$x^5 + 2x^2 + 2x + 2 = (x^2 + 1)(x^3 + 2x + 2)$$

over $\mathbb{Z}_3$ is

$$S = \{a_1 + a_2 u + a_3 v + a_4 uv + a_5 v^2 + a_6 uv^2 \mid a_i \in \mathbb{Z}_3\}$$

where $u^2 = 2$ and $v^3 = v + 1$. S can be obtained as

$$S = F[x]/\langle x^3 + 2x + 2\rangle$$

where $F = \mathbb{Z}_3[x]/\langle x^2 + 1\rangle$ or as

$$S = E[x]/\langle x^2 + 1\rangle$$

where $E = \mathbb{Z}_3[x]/\langle x^3 + 2x + 2\rangle$.

8 Algebraic extensions

$\mathbb{R}$ is an extension field of $\mathbb{Q}$ and $\mathbb{C}$ is an extension field of both $\mathbb{Q}$ and $\mathbb{R}$. However, the extensions of $\mathbb{C}$ over $\mathbb{R}$ and of $\mathbb{R}$ over $\mathbb{Q}$ are of a rather different nature.

Firstly, going from $\mathbb{R}$ to $\mathbb{C}$ is a small step, it suffices to adjoin a single element: $\mathbb{C} = \mathbb{R}(i)$. This cannot be done for $\mathbb{R}$ over $\mathbb{Q}$.

Secondly, there is no proper subfield between $\mathbb{R}$ and $\mathbb{C}$ whereas there are many different subfields between $\mathbb{Q}$ and $\mathbb{R}$, e.g., $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{3})$.

Can we distinguish any extension fields in a similar way? How many subfields are in between a field and an extension?

Definition 8.1 An extension of F of the form $F(a)$ is called a **simple** extension of F.

Example 8.2

1. $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ is a simple extension of $\mathbb{Q}$ because $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$.
2. $\mathbb{R}$ is not a simple extension of $\mathbb{Q}$.

Definition 8.3 Let E be an extension field of a field F and let $a \in E$. We call a **algebraic over** F if a is the zero of some nonzero polynomial in $F[x]$. If a is not algebraic over F, it is called **transcendental over** F.

Example 8.4

1. $\sqrt{2}$ and $\sqrt{2}+\sqrt{3}$ are algebraic over $\mathbb{Q}$.
2. π, Euler's number e and Liouville's constant $\sum_{n\geq 1} 10^{-n!}$ are transcendental over $\mathbb{Q}$.
3. π is algebraic over $\mathbb{Q}(\pi^3)$.

Definition 8.5 An extension E of F is called an **algebraic extension of** F if every element of E is algebraic over F. If E is not an algebraic extension of F, it is called a **transcendental** extension of F.

Example 8.6

1. $\mathbb{Q}(\sqrt{2})$ is an algebraic extension of $\mathbb{Q}$.
2. $\mathbb{R}$ is a transcendental extension of $\mathbb{Q}$.

3. $\mathbb{Q}(\pi)$ is an algebraic extension of $\mathbb{Q}(\pi^2)$.
4. $\mathbb{R}$ is a transcendental extension of $\mathbb{Q}(\pi)$.

Theorem 8.7 Let E be an extension field of a field F and let $a \in E$. If a is transcendental over F, then $F(a) \cong F(x)$, the field of quotients of $F[x]$, that is,

$$F(a) = \left\{ \frac{p(a)}{q(a)} \;\middle|\; p(x), q(x) \in F[x], q(x) \neq 0 \right\}.$$

If a is algebraic over F, then

$$F(a) \cong F[x]/\langle p(x) \rangle,$$

where $p(x)$ is a polynomial in $F[x]$ of minimum degree such that $p(a) = 0$. Moreover, $p(x)$ is irreducible over F and there is a unique monic irreducible polynomial $p(x)$ in $F[x]$ such that $p(a) = 0$.

Definition 8.8 Let E be an extension field of a field F and let $a \in E$ be algebraic over F. The polynomial $p(x)$ from Theorem 8.7 is called the **minimal polynomial for** a **over** F.

Example 8.9

1. The minimal polynomial for $\sqrt{2}$ over $\mathbb{Q}$ is $x^2 - 2$.
2. The minimal polynomial for $\sqrt{2} + \sqrt{3}$ over $\mathbb{Q}$ is $x^4 - 10x^2 + 1$.
3. The minimal polynomial for $\sqrt{1 + \sqrt[3]{2}}$ over $\mathbb{Q}$ is $x^6 - 3x^4 + 3x^2 - 3$.

Theorem 8.10 Let E be an extension field of a field F and let $a \in E$ be algebraic over F.
If $f(x) \in F[x]$ and $f(a) = 0$, then the minimal polynomial for a over F divides $f(x)$ in $F[x]$.

Definition 8.11 Let E be an extension field of a field F. We say that E **has degree** n **over** F and write $[E : F] = n$, if E has dimension n as a vector space over F. If $[E : F]$ is finite, E is called a **finite extension** of F; otherwise, we say that E is an **infinite extension** of F.

Example 8.12

1. $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$, $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$.
2. $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$.
3. $\mathbb{R}$ is an infinite extension of $\mathbb{Q}$.
4. If a is algebraic over F, then $[F(a) : F] = \deg m(x)$ where $m(x)$ is the minimal polynomial for a over F.

Theorem 8.13 If E is a finite extension of F, then E is an algebraic extension of F.

Theorem 8.14 (Degree formula)
Let K be a finite extension of the field E and let E be a finite extension of a field F. Then K is a finite extension of F, and

$$[K : F] = [K : E][E : F].$$

Example 8.15

1. $[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}] = [\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}(\sqrt{2})]\cdot[\mathbb{Q}(\sqrt{2}):\mathbb{Q}]$
   $= 2\cdot 2 = 4$
2. $x^2 - 3$ is irreducible over $\mathbb{Q}(\sqrt[3]{2})$.

Theorem 8.16 If K is an algebraic extension of E and E is an algebraic extension of F, then K is an algebraic extension of F.

Corollary 8.17 Let E be an extension field of a field F. Then the set of all elements of E that are algebraic over F is a subfield of E.

Definition 8.18 Let

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0 \in F[x].$$

The **derivative** for $f(x)$, denoted by $f'(x)$, is the polynomial

$$n a_n x^{n-1} + (n-1) a_{n-2} x^{n-1} + \ldots + a_1$$

in $F[x]$.

Theorem 8.19 Let $f(x), g(x) \in F[x]$ and $a \in F$. Then

1. $(f(x) + g(x))' = f'(x) + g'(x)$;
2. $(af(x))' = af'(x)$;
3. $(f(x)g(x))' = f'(x)g(x) + f(x)g'(x)$;
4. $(f(g(x)))' = f'(g(x))g'(x)$.

Theorem 8.20 A polynomial $f(x)$ over a field F has a multiple zero in some extension field E of F if and only if $f(x)$ and $f'(x)$ have a common factor of positive degree in $F[x]$.

Corollary 8.21 If $f(x)$ is an irreducible polynomial over a field F of characteristic 0, then $f(x)$ has no multiple zero.

Example 8.22 If F is a field of characteristic p, then $x^p - a \in F[x]$ is either irreducible over F or has a zero of multiplicity p in F.

Theorem 8.23 (Primitive Element Theorem, Steinitz, 1910)
If F is a field of characteristic 0, and a and b are algebraic over F, then there is an element c in $F(a,b)$ such that $F(a,b) = F(c)$.

Definition 8.24 If E is a finite extension of F, and a is an element of E with the property that $E = F(a)$, then a is called a **primitive element** of E.

Example 8.25

1. $\sqrt{2}+\sqrt{3}$ is a primitive element of $\mathbb{Q}(\sqrt{2},\sqrt{3})$.
2. $\mathbb{Q}(\sqrt{2},\sqrt[3]{2}) = \mathbb{Q}(\sqrt{2}+\sqrt[3]{2})$, but one also has $\mathbb{Q}(\sqrt{2},\sqrt[3]{2}) = \mathbb{Q}(\sqrt[6]{2})$.

Corollary 8.26 If F is a field of characteristic 0, and E is a finite extension of F, then E is a simple extension of F.

9 Finite fields

We know that $\mathbb{Z}_p$ where p is a prime is a field. We also encountered fields with, for example, 4 elements in Example 5.25 or 9 elements in Example 3.15.

Natural questions to ask are:

- What are all the finite fields?
- How can they be constructed?
- How many different finite fields of a given order are there?

Finite fields are important in, for example, coding theory and combinatorics. So knowledge of their structure is essential in these areas.

Theorem 9.1 A finite field has order p^n where p is a prime and n is a positive integer.

For each prime p and each positive integer n there is, up to isomorphism, a unique finite field of order p^n. This field, denoted by GF(p^n), is the **Galois field of order** p^n and can be obtained as the splitting field for $x^{p^n} - x$ over $\mathbb{Z}_p$.

As a group under addition GF(p^n) is isomorphic to $(\mathbb{Z}_p)^n$

$$\underbrace{\mathbb{Z}_p \oplus \mathbb{Z}_p \oplus \cdots \oplus \mathbb{Z}_p}_{n\ factors}.$$

and $[\mathrm{GF}(p^n) : \mathrm{GF}(p)] = n$. As a group under multiplication, the set GF$(p^n)^*$ of nonzero elements of GF(p^n) is isomorphic to $\mathbb{Z}_{p^n-1}$ and is, therefore, cyclic. If a is a generator of $\mathrm{GF}(p^n)^*$, then a is algebraic over $\mathrm{GF}(p)$ of degree n.
For each divisor m of n, $\mathrm{GF}(p^n)$ has a unique subfield of order p^m. Moreover, these are the only subfields of $\mathrm{GF}(p^n)$.

Example 9.2 x^3+x+1 and x^3+x^2+1 are two cubic irreducible polynomials over $\mathbb{Z}_2$. The fields

$$\begin{aligned}\mathbb{Z}_2(a) &\cong \mathbb{Z}_2[x]/\langle x^3+x^2+1\rangle \quad \text{and}\\ \mathbb{Z}_2(b) &\cong \mathbb{Z}_2[x]/\langle x^3+x+1\rangle\end{aligned}$$

where a is a root of x^3+x^2+1 and b is a root of x^3+x+1 are isomorphic. An isomorphism $\varphi : \mathbb{Z}_2(a) \to \mathbb{Z}_2(b)$ is given by $\varphi(r+sa+ta^2) = r+s+t+sb+tb^2$.

x^8-x splits in $\mathbb{Z}_2(a)$ as

$$\begin{aligned}x^8-x = {} & x(x+1)(x+a)(x+a+1)(x+a^2)\\ & (x+a^2+1)(x+a^2+a)\\ & (x+a^2+a+1).\end{aligned}$$

($x^8-x = x(x+1)(x^3+x+1)(x^3+x^2+1)$ over $\mathbb{Z}_2$.)

a is a generator of $\mathrm{GF}(8)^* \cong \mathbb{Z}_2(a)^*$.

Conversion Table for Addition and Multiplication in $\mathrm{GF}(8) \cong \mathbb{Z}_2(a)$

mult	add	add	mult
1	1	1	1
a	a	a	a
a^2	a^2	$a+1$	a^5
a^3	a^2+1	a^2	a^2
a^4	a^2+a+1	a^2+1	a^3
a^5	$a+1$	a^2+a	a^6
a^6	a^2+a	a^2+a+1	a^4

Example 9.3

1. $\mathrm{GF}(32)$ has no other proper subfield than $\mathbb{Z}_2$.
2. $\mathrm{GF}(64)$ has precisely three proper subfields, $\mathbb{Z}_2$, $\mathrm{GF}(4)$ and $\mathrm{GF}(8)$.

10 Geometric constructions

Using ruler and compass one can bisect a line segment and also an angle. One can easily construct equilateral triangles or regular hexagons. This kind of constructive mathematics was very important to ancient Greek mathematicians. They also posed problems like ‘Is it always possible to trisect an angle with ruler and compass’.

The general question is what points in the plane can be obtained by using ruler and compass, starting with two points that define a unit line segment.

Definition 10.1 A real number α is **constructible** if we can construct a line segment of length $|\alpha|$ in a finite number of steps from a given segment of unit length by using a ruler and compass.

Example 10.2

1. Each rational number is constructible.
2. $\sqrt{2}$ is constructible.

Theorem 10.3 If α and β are constructible real numbers, then so are $\alpha + \beta$, $\alpha - \beta$, $\alpha\beta$, α/β, if $\beta \neq 0$, and $\sqrt{\alpha}$, if $\alpha \geq 0$.
The set of all constructible real numbers forms a subfield F of the field of real numbers.

Theorem 10.4 The field F of constructible real numbers consists precisely of all real numbers that we can obtain from $\mathbb{Q}$ by taking square roots of positive numbers a finite number of times and applying a finite number of field operations. If $\gamma \notin \mathbb{Q}$ is constructible, then there is a finite sequence of real numbers $\alpha_1, \ldots, \alpha_n = \gamma$ such that $\mathbb{Q}(\alpha_1, \ldots, \alpha_i)$ is an extension of $\mathbb{Q}(\alpha_1, \ldots, \alpha_{i-1})$ of degree 2. In particular,

$$[\mathbb{Q}(\gamma) : \mathbb{Q}] = 2^r$$

for some integer $r \geq 0$.

Corollary 10.5 'Trisecting the angle is impossible', that is, there exists an angle that cannot be trisected with ruler and compass.

Corollary 10.6 ‘Doubling the cube is impossible’, that is, given a side of a cube, it is not always possible to construct with ruler and compass the side of a cube that has double the volume of the original cube.

Corollary 10.7 ‘Squaring the circle is impossible’, that is, given a circle, it is not always possible to construct with ruler and compass a square having area equal to the area of the given circle.

Theorem 10.8 **(Gauss, 1796)** It is possible to construct the regular n-gon with ruler and compass if and only if n has the form $2^k p_1 p_2 \cdots p_t$ where $k \geq 0$ and the p_i are distinct primes of the form $2^{2^m} + 1$ (Fermat primes).

Example 10.9 The regular 17-gon can be constructed by ruler and compass because

$$\cos\frac{2\pi}{17} = \frac{1}{16}\Bigg[-1 + \sqrt{17} + \sqrt{34 - 2\sqrt{17}} + \sqrt{68 + 12\sqrt{17} - 16\sqrt{34 + 2\sqrt{17}} - 2(1-\sqrt{17})\sqrt{34 - 2\sqrt{17}}}\Bigg]$$

Remark 10.10 In the quadratic, cubic or quartic formulas, the zeros for a quadratic, cubic or quartic polynomial, respectively, are expressed in terms of their coefficients and the use of square, cube or 4th roots.

For example, if F is a field of characteristic $\neq 2$, the quadratic polynomial $ax^2 + bx + c$ where $a, b, c \in F$, $a \neq 0$, has the zeros $\frac{1}{2a}\left(-b \pm \sqrt{b^2 - 4ac}\right) \in F\left(\sqrt{b^2 - 4ac}\right)$.

Similarly, the zeros of the cubic polynomial $ax^3 + bx^2 + cx + d$

where $a, b, c, d \in \mathbb{Q}$, $a \neq 0$, are

$$\frac{1}{3a}(-b + A + B), \frac{1}{6a}(-2b - A - B \pm (A - B)\sqrt{-3}),$$

where

$$A = \sqrt[3]{r + \sqrt{r^2 + s^3}}, \quad B = \sqrt[3]{r - \sqrt{r^2 + s^3}}$$

and

$$r = \frac{1}{2}(9abc - 2b^3 - 27a^2d), \quad s = 3ac - b^2.$$

The question is whether or not there are such formulas for equations for higher degrees, that is, whether or not such polynomials can be ‘solved by radicals’.

Using so-called Galois Theory one can show that there is no formula for solving general polynomial equations of degrees 5 and higher.