Abstract Algebra II

George Voutsadakis[1]

[1]Mathematics and Computer Science
Lake Superior State University

LSSU Math 342

Subsection 1

Basic Definitions and Examples

Rings, Commutative Rings and Rings with Identity

Definition (Ring)

(1) A **ring** R is a set together with two binary operations $+$ and $\times$ (called **addition** and **multiplication**) satisfying the following axioms:
   (i) $(R, +)$ is an abelian group;
   (ii) $\times$ is associative: $(a \times b) \times c = a \times (b \times c)$, for all $a, b, c \in R$;
   (iii) the distributive laws hold in R: for all $a, b, c \in R$,
   $(a + b) \times c = (a \times c) + (b \times c)$ and $a \times (b + c) = (a \times b) + (a \times c)$.

(2) The ring R is **commutative** if multiplication is commutative.

(3) The ring R is said to have an **identity** (or **contain a 1**) if there is an element $1 \in R$ with $1 \times a = a \times 1 = a$, for all $a \in R$.

- We usually write simply ab rather than $a \times b$, for $a, b \in R$.
- The additive identity of R will always be denoted by 0 and the additive inverse of the ring element a will be denoted by $-a$.

Division Rings and Fields

- Claim: If a ring R has a 1, then commutativity under addition follows by the distributive laws.

  Compute the product $(1+1)(a+b)$ in two different ways, using the distributive laws, but not assuming that addition is commutative:
  - $(1+1)(a+b) = 1(a+b)+1(a+b) = 1a+1b+1a+1b = a+b+a+b$;
  - $(1+1)(a+b) = (1+1)a+(1+1)b = 1a+1a+1b+1b = a+a+b+b$.

  Since R is a group under addition, this implies $b+a = a+b$, i.e., that R under addition is necessarily commutative.

Definition (Division Ring and Field)

A ring R with identity 1, where $1 \neq 0$, is called a **division ring** (or **skew field**) if every nonzero element $a \in R$ has a multiplicative inverse, i.e., there exists $b \in R$, such that $ab = ba = 1$.
A commutative division ring is called a **field**.

Examples I

(1) The simplest examples of rings are the **trivial rings** obtained by taking R to be any commutative group (denoting the group operation by $+$) and defining the multiplication $\times$ on R by $a \times b = 0$, for all $a, b \in R$.

It is easy to see that this multiplication defines a commutative ring. In particular, if $R = \{0\}$ is the trivial group, the resulting ring R is called the **zero ring**, denoted $R = 0$.

- Except for the zero ring, a trivial ring does not contain an identity ($R = 0$ is the only ring where $1 = 0$; we shall often exclude this ring by imposing the condition $1 \neq 0$).
- Trivial rings have two binary operations, but multiplication adds no new structure to the additive group.

(2) The ring of integers, $\mathbb{Z}$, under the usual operations of addition and multiplication is a commutative ring with identity (the integer 1). The ring axioms follow from the basic axioms for the system of natural numbers.

- Note that under multiplication $\mathbb{Z} - \{0\}$ is not a group.

Examples II

(3) Similarly, the rational numbers, $\mathbb{Q}$, the real numbers, $\mathbb{R}$, and the complex numbers, $\mathbb{C}$, are commutative rings with identity (actually fields).
The ring axioms for each of these follow ultimately from the ring axioms for $\mathbb{Z}$.

- We will construct $\mathbb{Q}$ from $\mathbb{Z}$.
- In field theory, one constructs $\mathbb{C}$ from $\mathbb{R}$.
- The construction of $\mathbb{R}$ from $\mathbb{Q}$ (and subsequent verification of the ring axioms) is the starting point in real analysis.

(4) The quotient group $\mathbb{Z}/n\mathbb{Z}$ is a commutative ring with identity (the element 1) under the operations of addition and multiplication of residue classes (frequently referred to as "modular arithmetic").
We saw that the additive abelian group axioms followed from the general principles of the theory of quotient groups.
We will see that the remaining ring axioms follow analogously from the general theory of quotient rings.

The Real Hamilton Quaternions

- An example of a noncommutative ring is a division ring discovered in 1843 by Sir William Rowan Hamilton:

(5) (The (**real**) **Hamilton Quaternions**) Let $\mathbb{H}$ be the collection of elements of the form $a+bi+cj+dk$, where $a,b,c,d \in \mathbb{R}$ are real numbers, where:

- addition is defined "componentwise" by

$$(a+bi+cj+dk)+(a'+b'i+c'j+d'k) \\ =(a+a')+(b+b')i+(c+c')j+(d+d')k;$$

- multiplication is defined by expanding $(a+bi+cj+dk)(a'+b'i+c'j+d'k)$ using the distributive law (being careful about the order of terms) and simplifying using the relations $i^2=j^2=k^2=-1$, $ij=-ji=k$, $jk=-kj=i$, $ki=-ik=j$ (where the real number coefficients commute with i,j and k).

Example: $(1+i+2j)(j+k)=1(j+k)+i(j+k)+2j(j+k)=$ $j+k+ij+ik+2j^2+2jk=j+k+k+(-j)+2(-1)+2(i)=-2+2i+2k.$

The Real Hamilton Quaternions (Cont'd)

- The fact that $\mathbb{H}$ is a ring may be proved by a straightforward, albeit lengthy, check of the axioms (associativity of multiplication is particularly tedious).
- The Hamilton Quaternions are a noncommutative ring with identity $(1 = 1 + 0i + 0j + 0k)$.
- Similarly, one can define the ring of **rational Hamilton Quaternions** by taking a, b, c, d to be rational numbers above.
- Both the real and rational Hamilton Quaternions are division rings, where inverses of nonzero elements are given by

$$(a + bi + cj + dk)^{-1} = \frac{a - bi - cj - dk}{a^2 + b^2 + c^2 + d^2}.$$

Rings of Functions

(6) Let X be any nonempty set and let A be any ring. The collection, R, of all (set) functions $f : X \to A$ is a ring under the usual definition of pointwise addition and multiplication of functions:

$$(f+g)(x) = f(x) + g(x) \quad \text{and} \quad (fg)(x) = f(x)g(x).$$

Each ring axiom for R follows from the corresponding axiom for A.

- The ring R is commutative if and only if A is commutative;
- R has a 1 if and only if A has a 1 (in which case the 1 of R is necessarily the constant function 1 on X).

- If X and A have more structure, we may form other rings of functions which respect those structures.

  For instance, if A is the ring of real numbers $\mathbb{R}$ and X is the closed interval $[0,1]$ in $\mathbb{R}$, we may form the ring of all continuous functions from $[0,1]$ to $\mathbb{R}$ (the basic limit theorems guarantee that sums and products of continuous functions are continuous).

  This is a commutative ring with 1.

Rings without Identity

(7) The ring $2\mathbb{Z}$ of even integers under usual addition and multiplication of integers (the sum and product of even integers is an even integer) is a ring without identity.

- A function $f : \mathbb{R} \to \mathbb{R}$ is said to have **compact support** if there are real numbers a, b (depending on f), such that $f(x) = 0$, for all $x \notin [a, b]$ (i.e., f is zero outside some bounded interval).

(8) The set of all functions $f : \mathbb{R} \to \mathbb{R}$ with compact support is a commutative ring without identity (since an identity could not have compact support).

Similarly, the set of all continuous functions $f : \mathbb{R} \to \mathbb{R}$ with compact support is a commutative ring without identity.

Basic Arithmetic in Rings

Proposition

Let R be a ring. Then:

(1) $0a = a0 = 0$, for all $a \in R$.

(2) $(-a)b = a(-b) = -(ab)$, for all $a, b \in R$ (recall $-a$ is the additive inverse of a).

(3) $(-a)(-b) = ab$, for all $a, b \in R$.

(4) If R has an identity 1, then the identity is unique and $-a = (-1)a$.

- These all follow from the distributive laws and cancelation in the additive group R.

(1) This follows from $0a = (0 + 0)a = 0a + 0a$.

(2) $(-a)b = -(ab)$ follows from $ab + (-a)b = (a + (-a))b = 0b = 0$.

- The rest follow similarly.
- Due to the distributive laws, the additive and multiplicative structures of a ring behave well with respect to one another, as in the integers.

Zero Divisors and Units

Definition (Zero Divisor and Unit)

Let R be a ring.

(1) A nonzero element a of R is called a **zero divisor** if there is a nonzero element b in R such that either $ab = 0$ or $ba = 0$.

(2) Assume R has an identity $1 \neq 0$. An element u of R is called a **unit** in R if there is some v in R, such that $uv = vu = 1$.
The set of units in R is denoted $R^{\times}$.

- The units in a ring R form a group under multiplication. So $R^{\times}$ will be referred to as the **group of units** of R.
- In this terminology a **field** is a commutative ring F with identity $1 \neq 0$ in which every nonzero element is a unit, i.e., $F^{\times} = F - \{0\}$.
- A zero divisor can never be a unit: Suppose a is a unit in R and $ab = 0$, for some nonzero b in R. Then $va = 1$ for some $v \in R$. so $b = 1b = (va)b = v(ab) = v0 = 0$, contradiction. Similarly if $ba = 0$.
- In particular, fields contain no zero divisors.

Examples I

(1) The ring $\mathbb{Z}$ of integers has no zero divisors and its only units are ± 1, i.e., $\mathbb{Z}^\times = \{\pm 1\}$. Note that every nonzero integer has an inverse in the larger ring $\mathbb{Q}$. So the property of being a unit depends on the ring in which an element is viewed.

(2) Let n be an integer ≥ 2. In the ring $\mathbb{Z}/n\mathbb{Z}$ the elements $\overline{u}$ for which u and n are relatively prime are units.

If, on the other hand, a is a nonzero integer and a is not relatively prime to n then we show that $\overline{a}$ is a zero divisor in $\mathbb{Z}/n\mathbb{Z}$:

Let d be the g.c.d. of a and n and let $b = \frac{n}{d}$. By assumption $d > 1$ so $0 < b < n$, i.e., $\overline{b} \neq \overline{0}$. By construction n divides ab, that is, $\overline{ab} = \overline{0}$ in $\mathbb{Z}/n\mathbb{Z}$. This shows that every nonzero element of $\mathbb{Z}/n\mathbb{Z}$ is either a unit or a zero divisor. Furthermore, every nonzero element is a unit if and only if every integer a in the range $0 < a < n$ is relatively prime to n. This happens if and only if n is a prime, i.e., $\mathbb{Z}/n\mathbb{Z}$ is a field if and only if n is a prime.

Examples II

(3) If R is the ring of all functions from the closed interval $[0, 1]$ to $\mathbb{R}$, then the units of R are the functions that are not zero at any point (for such f its inverse is the function $\frac{1}{f}$).

If f is not a unit and not zero, then f is a zero divisor:

Define $g(x) = \begin{cases} 0, & \text{if } f(x) \neq 0 \\ 1, & \text{if } f(x) = 0 \end{cases}$.

- g is not the zero function;
- $f(x)g(x) = 0$, for all x.

Continuous Functions from $[0,1]$ to $\mathbb{R}$

(4) If R is the ring of all continuous functions from the closed interval $[0,1]$ to $\mathbb{R}$, then the units of R are still the functions that are not zero at any point.

There are functions that are neither units nor zero divisors.

For instance, $f(x) = x - \frac{1}{2}$ has only one zero (at $x = \frac{1}{2}$) so f is not a unit. On the other hand, if $gf = 0$, then g must be zero for all $x \neq \frac{1}{2}$. But the only continuous function with this property is the zero function. Hence f is neither a unit nor a zero divisor.

Similarly, no function with only a finite (or countable) number of zeros on $[0,1]$ is a zero divisor.

This ring also contains many zero divisors.

For instance let $f(x) = \begin{cases} 0, & \text{if } 0 \leq x \leq \frac{1}{2} \\ x - \frac{1}{2}, & \text{if } \frac{1}{2} \leq x \leq 1 \end{cases}$ and let $g(x) = f(1-x)$. Then f and g are nonzero continuous functions whose product is the zero function.

Quadratic Fields

(5) Let D be a rational number that is not a perfect square in $\mathbb{Q}$ and define $\mathbb{Q}(\sqrt{D}) = \{a + b\sqrt{D} : a, b \in \mathbb{Q}\}$ as a subset of $\mathbb{C}$.

This set is clearly closed under subtraction. The identity $(a + b\sqrt{D})(c + d\sqrt{D}) = (ac + bdD) + (ad + bc)\sqrt{D}$ shows that it is also closed under multiplication. Hence $\mathbb{Q}(\sqrt{D})$ is a subring of $\mathbb{C}$ (even a subring of $\mathbb{R}$ if $D > 0$). In particular, it is a commutative ring with identity. The assumption that D is not a square implies that:

- Every element of $\mathbb{Q}(\sqrt{D})$ may be written uniquely in the form $a + b\sqrt{D}$;
- If a and b are not both 0 then $a^2 - Db^2$ is nonzero.

But $(a + b\sqrt{D})(a - b\sqrt{D}) = a^2 - Db^2$. Hence, if $a + b\sqrt{D} \neq 0$ (i.e., one of a or b is nonzero), then $\frac{a - b\sqrt{D}}{a^2 - Db^2}$ is the inverse of $a + b\sqrt{D}$ in $\mathbb{Q}(\sqrt{D})$. This shows that every nonzero element in this commutative ring is a unit. Thus, $\mathbb{Q}(\sqrt{D})$ is a field (called a **quadratic field**).

Quadratic Fields (Cont'd)

- The rational number D may be written $D = f^2 D'$, for some rational number f and a unique integer D', where D' is not divisible by the square of any integer greater than 1, i.e., D' is either -1 or ± 1 times the product of distinct primes in $\mathbb{Z}$ (for example, $\frac{8}{5} = (\frac{2}{5})^2 \cdot 10$). Call D' the **square free part** of D.
  - We have $\sqrt{D} = f\sqrt{D'}$.
  - Hence, $\mathbb{Q}(\sqrt{D}) = \mathbb{Q}(\sqrt{D'})$.

  Thus, we may assume that D is a square free integer in the definition of the quadratic field $\mathbb{Q}(\sqrt{D})$.

Integral Domains

Definition (Integral Domain)

A commutative ring with identity $1 \neq 0$ is called an **integral domain** if it has no zero divisors.

Proposition (Cancelation Property)

Assume a, b and c are elements of any ring with a not a zero divisor. If $ab = ac$, then either $a = 0$ or $b = c$ (i.e., if $a \neq 0$ we can cancel the a's). In particular, if a, b, c are any elements in an integral domain and $ab = ac$, then either $a = 0$ or $b = c$.

- If $ab = ac$, then $a(b - c) = 0$. So either $a = 0$ or $b - c = 0$.

  The second statement follows from the first and the definition of an integral domain.

Finite Integral Domains are Fieds

Corollary

Any finite integral domain is a field.

- Let R be a finite integral domain and let a be a nonzero element of R. By the cancelation law the map $x \mapsto ax$ is an injective function. Since R is finite this map is also surjective. In particular, there is some $b \in R$, such that $ab = 1$, i.e., a is a unit in R. Since a was an arbitrary nonzero element, R is a field.
- A remarkable result of Wedderburn is that a finite division ring is necessarily commutative, i.e., is a field.

Subrings

Definition (Subring)

A **subring** of the ring R is a subgroup of R that is closed under multiplication.

- In other words, a subset S of a ring R is a subring if the operations of addition and multiplication in R when restricted to S give S the structure of a ring.
- To show that a subset of a ring R is a subring it suffices to check that:
  - it is nonempty;
  - it is closed under subtraction;
  - it is closed under multiplication.

Examples of Subrings

(1) $\mathbb{Z}$ is a subring of $\mathbb{Q}$ and $\mathbb{Q}$ is a subring of $\mathbb{R}$.
The property "is a subring of" is clearly transitive.

(2) $2\mathbb{Z}$ is a subring of $\mathbb{Z}$, as is $n\mathbb{Z}$, for any integer n.
The ring $\mathbb{Z}/n\mathbb{Z}$ is not a subring (or a subgroup) of $\mathbb{Z}$, for any $n \geq 2$.

(3) The ring of all continuous functions from $\mathbb{R}$ to $\mathbb{R}$ is a subring of the ring of all functions from $\mathbb{R}$ to $\mathbb{R}$.
The ring of all differentiable functions from $\mathbb{R}$ to $\mathbb{R}$ is a subring of both of these.

(4) $S = \mathbb{Z} + \mathbb{Z}i + \mathbb{Z}j + \mathbb{Z}k$, the **integral Quaternions**, form a subring of either the real or the rational Quaternions.
This ring (which is not a division ring) can be used to give proofs for a number of results in number theory.

(5) If R is a subring of a field F that contains the identity of F then R is an integral domain. The converse of this is also true: Any integral domain is contained in a field.

Subsection 2

Polynomial Rings, Matrix Rings and Group Rings

Polynomial Rings

- Fix a commutative ring R with identity. Let x be an indeterminate.
- The formal sum

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

  with $n \geq 0$ and each $a_i \in R$, is called a **polynomial** in x with coefficients a_i in R.
- If $a_n \neq 0$, then the polynomial is said to be of **degree** n, $a_n x^n$ is called the **leading term**, and a_n is called the **leading coefficient** (where the leading coefficient of the zero polynomial is taken to be 0).
- The polynomial is **monic** if $a_n = 1$.
- The set of all such polynomials is called the ring of **polynomials in the variable** x **with coefficients in** R and will be denoted $R[x]$.

Operations in $R[x]$

- The operations of addition and multiplication which make $R[x]$ into a ring are the same operations familiar from elementary algebra:
  - Addition is "componentwise":
    $(a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0) + (b_n x^n + b_{n-1}x^{n-1} + \cdots + b_1 x + b_0) =$
    $(a_n + b_n)x^n + (a_{n-1} + b_{n-1})x^{n-1} + \cdots + (a_1 + b_1)x + (a_0 + b_0)$ (here a_n or b_n may be zero in order for addition of polynomials of different degrees to be defined).
  - For multiplication:
    - first define $(ax^i)(bx^j) = abx^{i+j}$, for polynomials with one nonzero term,
    - then extend to all polynomials by the distributive laws ("expanding out and collecting like terms"):
      $(a_0 + a_1 x + a_2 x^2 + \cdots) \times (b_0 + b_1 x + b_2 x^2 + \cdots) =$
      $a_0 b_0 + (a_0 b_l + a_1 b_0)x + (a_0 b_2 + a_1 b_1 + a_2 b_0)x^2 + \cdots$ (in general, the coefficient of x^k in the product will be $\sum_{i=0}^{k} a_i b_{k-i}$).
- $R[x]$ is a ring with these definitions of addition and multiplication.
- The ring R appears in $R[x]$ as the **constant polynomials**.
- By definition, $R[x]$ is a commutative ring with the identity 1 from R.

Examples of Polynomial Rings

- If the coefficient ring R is the integers $\mathbb{Z}$ (respectively, the rationals $\mathbb{Q}$) the polynomial ring $\mathbb{Z}[x]$ (respectively, $\mathbb{Q}[x]$) is the ring of polynomials with integer (rational) coefficients familiar from elementary algebra.
- Another example is the polynomial ring $\mathbb{Z}/3\mathbb{Z}[x]$ of polynomials in x with coefficients in $\mathbb{Z}/3\mathbb{Z}$.

  This ring consists of nonnegative powers of x with coefficients $0, 1$ and 2 with calculations on the coefficients performed modulo 3.

  E.g., if $p(x) = x^2 + 2x + 1$ and $q(x) = x^3 + x + 2$, then $p(x) + q(x) = x^3 + x^2$ and $p(x)q(x) = x^5 + 2x^4 + 2x^3 + x^2 + 2x + 2$.
- The ring in which the coefficients are taken makes a substantial difference in the behavior of polynomials:

  E.g., the polynomial $x^2 + 1$ is not a perfect square in the polynomial ring $\mathbb{Z}[x]$, but is a perfect square in the polynomial ring $\mathbb{Z}/2\mathbb{Z}[x]$, since, in this ring, $(x + 1)^2 = x^2 + 2x + 1 = x^2 + 1$.

Properties of Polynomial Rings over Integral Domains

Proposition

Let R be an integral domain and let $p(x), q(x)$ be nonzero elements of $R[x]$. Then:

(1) $\text{degree} p(x)q(x) = \text{degree} p(x) + \text{degree} q(x)$;

(2) the units of $R[x]$ are just the units of R;

(3) $R[x]$ is an integral domain.

- If R has no zero divisors, then neither does $R[x]$: if $p(x)$ and $q(x)$ are polynomials with leading terms $a_n x^n$ and $b_m x^m$, respectively, then the leading term of $p(x)q(x)$ is $a_n b_m x^{n+m}$, and $a_n b_m \neq 0$. This proves (3) and also verifies (1).
  Suppose $p(x)$ is a unit. Then $p(x)q(x) = 1$ for some $q(x) \in R[x]$. Hence, $\text{degree} p(x) + \text{degree} q(x) = 0$. So both $p(x)$ and $q(x)$ are elements of R. Thus, they are units in R, since their product is 1. This proves (2).

Additional Properties of Polynomial Rings

- If the ring R has zero divisors then so does $R[x]$, because $R \subseteq R[x]$.
- Also, if $f(x)$ is a zero divisor in $R[x]$ (i.e., $f(x)g(x) = 0$, for some nonzero $g(x) \in R[x]$) then in fact $cf(x) = 0$, for some nonzero $c \in R$.
- Examples of Subrings of Polynomial Rings:
  - If S is a subring of R then $S[x]$ is a subring of $R[x]$.
    E.g., $\mathbb{Z}[x]$ is a subring of $\mathbb{Q}[x]$.
  - The set of all polynomials in x^2 (i.e., in which only even powers of x appear) form a subring of $R[x]$.
  - The set of all polynomials with zero constant term form a subring of $R[x]$ without an identity.

Matrix Rings

- Fix an arbitrary ring R and let n be a positive integer.
- Let $M_n(R)$ be the set of all $n \times n$ matrices with entries from R.
- The element (a_{ij}) of $M_n(R)$ is an $n \times n$ square array of elements of R whose entry in row i and column j is $a_{ij} \in R$.
- The set of matrices becomes a ring under the usual rules by which matrices of real numbers are added and multiplied:
  - Addition is componentwise: the i, j entry of $(a_{ij}) + (b_{ij})$ is $a_{ij} + b_{ij}$.
  - The i, j entry of the matrix product $(a_{ij}) \times (b_{ij})$ is $\sum_{k=1}^{n} a_{ik} b_{kj}$.

  These operations make $M_n(R)$ into a ring.
- It is called the **ring of $n \times n$ matrices with entries from R**.

Non Commutativity of Matrix Rings

- If R is any nontrivial ring and $n \geq 2$, then $M_n(R)$ is not commutative:

  Suppose $ab \neq 0$ in R.

  Let A be the matrix with a in position $1,1$ and zeros elsewhere

$$A = \begin{pmatrix} a & 0 & 0 & \cdots \\ 0 & 0 & 0 & \cdots \\ \vdots & \vdots & \vdots & \ddots \end{pmatrix} \qquad B = \begin{pmatrix} 0 & b & 0 & \cdots \\ 0 & 0 & 0 & \cdots \\ \vdots & \vdots & \vdots & \ddots \end{pmatrix}$$

  Let B be the matrix with b in position $1,2$ and zeros elsewhere;

  Then ab is the (nonzero) entry in position $1,2$ of AB, whereas BA is the zero matrix.

  These two matrices also show that $M_n(R)$ has zero divisors for all nonzero rings R whenever $n \geq 2$.

Scalar Matrices

- An element (a_{ij}) of $M_n(R)$ is called a **scalar matrix** if for some $a \in R$, $a_{ii} = a$, for all $i \in \{1, \ldots, n\}$, and $a_{ij} = 0$, for all $i \neq j$ (i.e., all diagonal entries equal a and all off-diagonal entries are 0).
- The set of scalar matrices is a subring of $M_n(R)$.
  This subring is a copy of R (i.e., is "isomorphic" to R): if the matrix A has the element a along the main diagonal and the matrix B has the element b along the main diagonal then:
  - the matrix $A + B$ has $a + b$ along the diagonal;
  - AB has ab along the diagonal (and all other entries 0).
- If R is commutative, the scalar matrices commute with all elements of $M_n(R)$.
- If R has a 1, then the scalar matrix with 1's down the diagonal (the $n \times n$ identity matrix) is the 1 of $M_n(R)$.
  In this case the units in $M_n(R)$ are the invertible $n \times n$ matrices.
  The group of units is denoted $\mathrm{GL}_n(R)$, the **general linear group of degree n over R**.

Subrings of Matrices

- If S is a subring of R then $M_n(S)$ is a subring of $M_n(R)$.

  For instance $M_n(\mathbb{Z})$ is a subring of $M_n(\mathbb{Q})$ and $M_n(2\mathbb{Z})$ is a subring of both of these.
- Another example of a subring of $M_n(\mathbb{R})$ is the set of upper triangular matrices:

$$\{(a_{ij}) : a_{pq} = 0 \text{ whenever } p > q\}$$

  (the set of matrices all of whose entries below the main diagonal are zero).

  One easily checks that the sum and product of upper triangular matrices is upper triangular.

Group Rings

- Fix a commutative ring R with identity $1 \neq 0$ and $G = \{g_1, g_2, \ldots, g_n\}$ be any finite group with group operation written multiplicatively.
- Define the **group ring**, RG, of G with coefficients in R, to be the set of all formal sums

$$a_1g_1 + a_2g_2 + \cdots + a_ng_n, \ a_i \in R, \ 1 \leq i \leq n.$$

- If g_1 is the identity of G we shall write a_1g_1 simply as a_1.
- Similarly, we shall write the element $1g$ for $g \in G$ simply as g.
  - Addition is defined "componentwise":
    $(a_1g_1 + a_2g_2 + \cdots + a_ng_n) + (b_1g_1 + a_2g_2 + \cdots + b_ng_n) =$
    $(a_1 + b_1)g_1 + (a_2 + b_2)g_2 + \cdots + (a_n + b_n)g_n$.
  - Multiplication is performed by:
    - first defining $(ag_i)(bg_j) = (ab)g_k$, where the product ab is taken in R and $g_ig_j = g_k$ is the product in the group G;
    - This product is then extended to all formal sums by the distributive laws so that the coefficient of g_k in the product $(a_1g_1 + \cdots + a_ng_n) \times (b_1g_1 + \cdots + b_ng_n)$ is $\sum_{g_ig_j=g_k} a_ib_j$.

Group Rings (Cont'd)

- It is straightforward to check that these operations make RG into a ring (again, commutativity of R is not needed).
  The associativity of multiplication follows from the associativity of the group operation in G.
- The ring RG is commutative if and only if G is a commutative group.
  Example: Let $G = D_8$ be the dihedral group of order 8 with the usual generators r, s ($r^4 = s^2 = 1$ and $rs = sr^{-1}$) and let $R = \mathbb{Z}$.
  The elements $\alpha = r + r^2 - 2s$ and $\beta = -3r^2 + rs$ are typical members of $\mathbb{Z}D_8$. Their sum and product are then

$$\begin{aligned}
\alpha + \beta &= r - 2r^2 - 2s + rs; \\
\alpha\beta &= (r + r^2 - 2s)(-3r^2 + rs) \\
&= r(-3r^2 + rs) + r^2(-3r^2 + rs) - 2s(-3r^2 + rs) \\
&= -3r^3 + r^2s - 3 + r^3s + 6r^2s - 2r^3 \\
&= -3 - 5r^3 + 7r^2s + r^3s.
\end{aligned}$$

R as a Subring and G as a Subgroup of the Units of RG

- The ring R appears in RG as the "constant" formal sums, i.e., the R-multiples of the identity of G (addition and multiplication in RG restricted to these elements is just addition and multiplication in R).

  These elements of R commute with all elements of RG.

  The identity of R is the identity of RG.
- The group G also appears in RG (the element g_i appears as $1g_i$).

  Example: $r, s \in D_8$ are also elements of the group ring $\mathbb{Z}D_8$ above.

  Multiplication in the ring RG restricted to G is just the group operation.

  In particular, each element of G has a multiplicative inverse in the ring RG (namely, its inverse in G).

  Thus, G is a subgroup of the group of units of RG.

Zero-Divisors in Group Rings

- If $|G| > 1$, then RG always has zero divisors:
  Let g be any element of G of order $m > 1$. Then

$$\begin{aligned}(1-g)(1+g+\cdots+g^{m-1}) &= 1-g^m \\ &= 1-1 \\ &= 0.\end{aligned}$$

  In RG neither of the formal sums in the above product is zero.

  Hence, $1-g$ is a zero divisor.

Subrings of Group Rings

- If S is a subring of R, then SG is a subring of RG.

  Example: $\mathbb{Z}G$ (called the **integral group ring of** G) is a subring of $\mathbb{Q}G$ (the **rational group ring of** G).
- Furthermore, if H is a subgroup of G then RH is a subring of RG.
- The set of all elements of RG whose coefficients sum to zero is a subring (without identity).
- If $|G| > 1$, the set of elements with zero "constant term" (i.e., the coefficient of the identity of G is zero) is not a subring (it is not closed under multiplication).

$\mathbb{R}Q_8$ versus $\mathbb{H}$

- Note that the group ring $\mathbb{R}Q_8$ is not the same ring as the Hamilton Quaternions $\mathbb{H}$ even though the latter contains a copy of the quaternion group Q_8 (under multiplication).
  - One difference is that the unique element of order 2 in Q_8 (usually denoted by -1) is not the additive inverse of 1 in $\mathbb{R}Q_8$.
    In other words, if we temporarily denote the identity of the group Q_8 by g_1 and the unique element of order 2 by g_2, then $g_1 + g_2$ is not zero in $\mathbb{R}Q_8$, whereas $1 + (-1)$ is zero in $\mathbb{H}$.
  - Furthermore, as noted above, the group ring $\mathbb{R}Q_8$ contains zero divisors;
    Hence $\mathbb{R}Q_8$ is not a division ring.

Subsection 3

Ring Homomorphisms and Quotient Rings

Ring Homomorphisms

Definition (Ring Homomorphism)

Let R and S be rings.

(1) A **ring homomorphism** is a map $\varphi : R \to S$ satisfying
   (i) $\varphi(a+b) = \varphi(a) + \varphi(b)$, for all $a, b \in R$ (so φ is a group homomorphism on the additive groups);
   (ii) $\varphi(ab) = \varphi(a)\varphi(b)$, for all $a, b \in R$.

(2) The **kernel** of the ring homomorphism φ, denoted $\ker\varphi$, is the set of elements of R that map to 0 in S (i.e., the kernel of φ viewed as a homomorphism of additive groups).

(3) A bijective ring homomorphism is called an **isomorphism**.

- If the context is clear, we shall simply use the term "homomorphism" instead of "ring homomorphism".
- Similarly, if A and B are rings, $A \cong B$ will always mean an isomorphism of rings unless otherwise stated.

Examples I

(1) The map $\varphi : \mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$ defined by sending an even integer to 0 and an odd integer to 1 is a ring homomorphism.

- The map is additive since the sum of two even or odd integers is even and the sum of an even integer and an odd integer is odd.
- The map is multiplicative since the product of two odd integers is odd and the product of an even integer with any integer is even.

The kernel of φ (the fiber of φ above $0 \in \mathbb{Z}/2\mathbb{Z}$) is the set of even integers.

The fiber of φ above $1 \in \mathbb{Z}/2\mathbb{Z}$ is the set of odd integers.

Examples II

(2) For $n \in \mathbb{Z}$ the maps $\varphi_n : \mathbb{Z} \to \mathbb{Z}$ defined by $\varphi_n(x) = nx$ are not in general ring homomorphisms because $\varphi_n(xy) = nxy$ whereas $\varphi_n(x)\varphi_n(y) = nxny = n^2xy$.
Hence φ_n is a ring homomorphism only when $n^2 = n$, i.e., $n = 0, 1$.

- φ_n is always a group homomorphism on the additive groups.
- φ_0 is the zero homomorphism and φ_1 is the identity homomorphism.

(3) Let $\varphi : \mathbb{Q}[x] \to \mathbb{Q}$ be the map from the ring of polynomials in x with rational coefficients to the rationals defined by $\varphi(p(x)) = p(0)$ (i.e., mapping the polynomial to its constant term).
Then φ is a ring homomorphism:

- The constant term of the sum is the sum of their constant terms;
- The constant term of the product is the product of their constant terms.

- The fiber above $a \in \mathbb{Q}$ consists of the set of polynomials with a as constant term.
- The kernel consists of the polynomials with constant term 0.

The Kernel and the Image of a Ring Homomorphism

Proposition

Let R and S be rings and let $\varphi : R \to S$ be a homomorphism.

(1) The image of φ is a subring of S.

(2) The kernel of φ is a subring of R. Furthermore, if $\alpha \in \ker\varphi$ then $r\alpha$ and $\alpha r \in \ker\varphi$, for every $r \in R$, i.e., $\ker\varphi$ is closed under multiplication by elements from R.

(1) If $s_1, s_2 \in \text{im}\varphi$, then $s_1 = \varphi(r_1)$ and $s_2 = \varphi(r_2)$, for some $r_1, r_2 \in R$. Then $\varphi(r_1 - r_2) = s_1 - s_2$ and $\varphi(r_1 r_2) = s_1 s_2$. This shows $s_1 - s_2, s_1 s_2 \in \text{im}\varphi$. So the image of φ is closed under subtraction and under multiplication. Hence, it is a subring of S.

(2) If $\alpha, \beta \in \ker\varphi$, then $\varphi(\alpha) = \varphi(\beta) = 0$. Hence $\varphi(\alpha - \beta) = 0$ and $\varphi(\alpha\beta) = 0$. So $\ker\varphi$ is closed under subtraction and under multiplication. Hence, it is a subring of R.
Similarly, for any $r \in R$, we have $\varphi(r\alpha) = \varphi(r)\varphi(\alpha) = \varphi(r)0 = 0$.
Also $\varphi(ar) = \varphi(\alpha)\varphi(r) = 0\varphi(r) = 0$. So $r\alpha, \alpha r \in \ker\varphi$.

The Quotient Ring

- Let $\varphi : R \to S$ be a ring homomorphism with kernel I.
- Since $\varphi : R \to S$ is a homomorphism of abelian groups, if r is any element of R mapping to $a \in S$, $\varphi(r) = a$, then the fiber of φ over a is the coset $r + I$ of the kernel I.
- If X is the fiber over $a \in S$ and Y is the fiber over $b \in S$, then:
  - $X + Y$ is the fiber over $a + b$;
  - XY is the fiber over ab.
- In terms of cosets of the kernel I this addition and multiplication is:
  - $(r + I) + (s + I) = (r + s) + I$;
  - $(r + I) \times (s + I) = (rs) + I$.
- These operations define a ring structure on the collection of cosets of the kernel I. This ring of cosets is called the **quotient ring of R by $I = \ker\varphi$** and is denoted R/I.
- The additive structure of the ring R/I is just the additive quotient group of the additive abelian group R by the (necessarily normal) subgroup I.

Necessary Conditions for Defining Multiplication in R/I

- Let I be an arbitrary subgroup of the additive group R.
- For the multiplication of cosets $(r+I)\times(s+I)=(rs)+I$ to be well defined and make the additive abelian group R/I into a ring, it must be independent of the particular representatives r and s chosen:

  I.e., if instead we use the representatives $r+\alpha$ and $s+\beta$, for any $\alpha,\beta\in I$, we must have

  $$(r+\alpha)(s+\beta)+I=rs+I,$$

  for all $r,s\in R$ and all $\alpha,\beta\in I$.
  - Letting $r=s=0$, we see that I must be closed under multiplication, i.e., I must be a subring of R.
  - By letting $s=0$ and letting r be arbitrary, we see that we must have $r\beta\in I$ for every $r\in R$ and every $\beta\in I$, i.e., that I must be closed under multiplication on the left by elements from R.
  - Letting $r=0$ and letting s be arbitrary, we see similarly that I must be closed under multiplication on the right by elements from R.

Sufficiency of the Condition

- If I is closed under multiplication on the left and on the right by elements from R then

$$(r+\alpha)(s+\beta)+I = rs+I$$

  is satisfied for all $\alpha, \beta \in I$.
- This shows that this is a necessary and sufficient condition for the multiplication to be well defined.

The Quotient Ring

- If the multiplication of cosets defined by
$$(r+I)\times(s+I)=(rs)+I$$
is well defined, then this multiplication makes the additive quotient group R/I into a ring.
- Each ring axiom in the quotient follows directly from the corresponding axiom in R.
Example: One of the distributive laws is verified as follows:
$$\begin{aligned}(r+I)[(s+I)+(t+I)] &= (r+I)[(s+t)+I]\\ &= r(s+t)+I=(rs+rt)+I\\ &= (rs+I)+(rt+I)\\ &= [(r+I)(s+I)]+[(r+I)(t+I)].\end{aligned}$$
- The quotient R/I of R by a subgroup I has a natural ring structure if and only if I is also closed under multiplication on the left and on the right by elements from R (in particular, I must be a subring of R).

Ideals

Definition (Ideal)

Let R be a ring, let I be a subset of R and let $r \in R$.

(1) $rI = \{ra : a \in I\}$ and $Ir = \{ar : a \in I\}$.

(2) A subset I of R is a **left ideal** of R if

- (i) I is a subring of R;
- (ii) I is closed under left multiplication by elements from R, i.e., $rI \subseteq I$, for all $r \in R$.

Similarly I is a **right ideal** if (i) holds and in place of (ii) one has

- (ii)′ I is closed under right multiplication by elements from R, i.e., $Ir \subseteq I$, for all $r \in R$.

(3) A subset I that is both a left ideal and a right ideal is called an **ideal** (or, for added emphasis, a **two-sided ideal**) of R.

- For commutative rings the notions of left, right and two-sided ideal coincide.

Remarks on Ideals

- To prove a subset I of a ring R is an ideal it is necessary to prove that:
  - I is nonempty;
  - I is closed under subtraction;
  - I is closed under multiplication by all the elements of R (and not just by elements of I).
- If R has a 1 then $(-1)a = -a$;

  So in this case I is an ideal if it is:
  - nonempty;
  - closed under addition;
  - closed under multiplication by all the elements of R.
- The kernel of any ring homomorphism is an ideal.

The Quotient Ring by an Ideal

Proposition

Let R be a ring and let I be an ideal of R. Then the (additive) quotient group R/I is a ring under the binary operations:

$$(r+I)+(s+I)=(r+s)+I \quad \text{and} \quad (r+I)\times(s+I)=(rs)+I,$$

for all $r, s \in R$. Conversely, if I is any subgroup such that the above operations are well defined, then I is an ideal of R.

Definition (Quotient Ring)

When I is an ideal of R, the ring R/I with the operations in the previous proposition is called the **quotient ring of R by I**.

The First Isomorphism Theorem

Theorem

(1) (**The First Isomorphism Theorem for Rings**) If $\varphi : R \to S$ is a homomorphism of rings, then the kernel of φ is an ideal of R, the image of φ is a subring of S and $R/\ker\varphi$ is isomorphic as a ring to $\varphi(R)$.

(2) If I is any ideal of R, then the map $R \to R/I$ defined by $r \mapsto r + I$ is a surjective ring homomorphism with kernel I (this homomorphism is called the **natural projection** of R onto R/I). Thus, every ideal is the kernel of a ring homomorphism and vice versa.

- If I is the kernel of φ, then the cosets (under addition) of I are precisely the fibers of φ. In particular, the cosets $r + I, s + I$ and $rs + I$ are the fibers of φ over $\varphi(r), \varphi(s)$ and $\varphi(rs)$, respectively. Since φ is a ring homomorphism $\varphi(r)\varphi(s) = \varphi(rs)$. Hence, $(r + I)(s + I) = rs + I$. Multiplication of cosets is well defined and so I is an ideal and R/I is a ring.

The First Isomorphism Theorem (Cont'd)

- The correspondence $r + I \mapsto \varphi(r)$ is a bijection between the rings R/I and $\varphi(R)$ which respects addition and multiplication. Hence, it is a ring isomorphism.

  If I is any ideal, then R/I is a ring (in particular is an abelian group) and the map $\pi : r \mapsto r + I$ is a group homomorphism with kernel I. It remains to check that π is a ring homomorphism. This is immediate from the definition of multiplication in R/I:

$$\pi : rs \mapsto rs + I = (r + I)(s + I) = \pi(r)\pi(s).$$

- As with groups we shall often use the bar notation for reduction mod $I : \overline{r} = r + I$. With this notation the addition and multiplication in the quotient ring R/I become simply:
  - $\overline{r} + \overline{s} = \overline{r + s}$;
  - $\overline{r}\ \overline{s} = \overline{rs}$.

Proper Ideals and the Integers Modulo n

- Let R be a ring.
  (1) The subrings R and $\{0\}$ are ideals. An ideal I is **proper** if $I \neq R$. The ideal $\{0\}$ is called the **trivial ideal** and is denoted by 0.
  (2) $n\mathbb{Z}$ is an ideal of $\mathbb{Z}$, for any $n \in \mathbb{Z}$. These are the only ideals of $\mathbb{Z}$, since in particular these are the only subgroups of $\mathbb{Z}$. The associated quotient ring is $\mathbb{Z}/n\mathbb{Z}$.
  E.g., if $n = 15$, then the elements of $\mathbb{Z}/15\mathbb{Z}$, are the cosets $\overline{0}, \overline{1}, \ldots, \overline{13}, \overline{14}$. To add (or multiply) in the quotient:
    - Choose any representatives for the two cosets;
    - Add (multiply, respectively) these representatives in the integers $\mathbb{Z}$;
    - Take the corresponding coset containing this sum (product, respectively).

  For example, in $\mathbb{Z}/15\mathbb{Z}$, $\overline{7} + \overline{11} = \overline{18} = \overline{3}$. We could also express this by writing $7 + 11 = 3 \mod 15$.
  The natural projection $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ is called **reduction mod** n.

Polynomials of Degree at Least 2

(3) Let $R = \mathbb{Z}[x]$ be the ring of polynomials in x with integer coefficients. Let I be the collection of polynomials whose terms are of degree at least 2 (i.e., having no terms of degree 0 or degree 1), together with the zero polynomial. Then I is an ideal:

- The sum of two such polynomials again has terms of degree at least 2;
- The product of a polynomial whose terms are of degree at least 2 with any polynomial again only has terms of degree at least 2.

Two polynomials $p(x), q(x)$ are in the same coset of I if and only if they differ by a polynomial whose terms are of degree at least 2, i.e., if and only if $p(x)$ and $q(x)$ have the same constant and first degree terms.

E.g, the polynomials $3 + 5x + x^3 + x^5$ and $3 + 5x - x^4$ are in the same coset of I.

It follows that a complete set of representatives for the quotient R/I is given by the polynomials $a + bx$ of degree at most 1.

Polynomials of Degree at Least 2 (Cont'd)

(3) Addition and multiplication in the quotient are again performed by representatives: For example,

$$(\overline{1+3x})+(\overline{-4+5x})=\overline{-3+8x}$$

and

$$(\overline{1+3x})(\overline{-4+5x})=(\overline{-4-7x+15x^2})=\overline{-4-7x}.$$

Note that in this quotient ring R/I, we have $\overline{x}\,\overline{x}=\overline{x^2}=\overline{0}$.
So R/I has zero divisors, even though $R=\mathbb{Z}[x]$ does not.

Ideal of a Ring of Functions

(4) Let A be a ring, let X be any nonempty set and let R be the ring of all functions from X to A.

For each fixed $c \in X$ the map $E_c : R \to A$, defined by

$$E_c(f) = f(c)$$

(called **evaluation at** c) is a ring homomorphism because the operations in R are pointwise addition and multiplication of functions.

The kernel of E_c is given by $\{f \in R : f(c) = 0\}$ (the set of functions from X to A that vanish at c).

Also, E_c is surjective: given any $a \in A$, the constant function $f(x) = a$ maps to a under evaluation at e. Thus $R/\ker E_c \cong A$.

Ideal of a Ring of Functions (Cont'd)

(4) Similarly, let X be the closed interval $[0,1]$ in $\mathbb{R}$ and let R be the ring of all continuous real valued functions on $[0,1]$.

For each $c \in [0,1]$, evaluation at c is a surjective ring homomorphism (since R contains the constant functions) and so $R/\ker E_c \cong \mathbb{R}$.

- The kernel of E_c is the ideal of all continuous functions whose graph crosses the x-axis at c.
- The fiber of E_c above $y_0 \in \mathbb{R}$ is the set of all continuous functions that pass through the point (c, y_0).

Evaluation of a Polynomial at 0

(5) The map from the polynomial ring $R[x]$ to R defined by $p(x) \mapsto p(0)$ (**evaluation at** 0) is a ring homomorphism whose kernel is the set of all polynomials whose constant term is zero, i.e., $p(0) = 0$.

We can compose this homomorphism with any homomorphism from R to another ring S to obtain a ring homomorphism from $R[x]$ to S.

E.g., let $R = \mathbb{Z}$ and consider the homomorphism $\mathbb{Z}[x] \to \mathbb{Z}/2\mathbb{Z}$, defined by the composition

$$p(x) \mapsto p(0) \mapsto p(0) \mod 2 \in \mathbb{Z}/2\mathbb{Z}.$$

- The kernel of the composite is $\{p(x) \in \mathbb{Z}[x] : p(0) \in 2\mathbb{Z}\}$, i.e., the set of all polynomials with integer coefficients whose constant term is even.
- The other fiber of this homomorphism is the coset of polynomials whose constant term is odd, as we determined earlier.

Since the homomorphism is surjective, the quotient ring is $\mathbb{Z}/2\mathbb{Z}$.

Ideal of a Ring of Matrices

(6) Fix some $n \in \mathbb{Z}$, with $n \geq 2$, and consider the noncommutative ring $M_n(R)$.

If J is any ideal of R, then $M_n(J)$, the $n \times n$ matrices whose entries come from J, is a two-sided ideal of $M_n(R)$.

This ideal is the kernel of the surjective homomorphism $M_n(R) \to M_n(R/J)$ which reduces each entry of a matrix mod J, i.e., which maps each entry a_{ij} to $\overline{a_{ij}}$ (bar denotes passage to R/J).

E.g., when $n = 3$ and $R = \mathbb{Z}$, the 3×3 matrices whose entries are all even is the two-sided ideal $M_3(2\mathbb{Z})$ of $M_3(\mathbb{Z})$ and the quotient $M_3(\mathbb{Z})/M_3(2\mathbb{Z})$ is isomorphic to $M_3(\mathbb{Z}/2\mathbb{Z})$.

If the ring R has an identity, then every two-sided ideal of $M_n(R)$ is of the form $M_n(J)$ for some two-sided ideal J of R.

Ideals of a Group Ring

(7) Let R be a commutative ring with 1 and let $G = \{g_1, \ldots, g_n\}$ be a finite group.
The map from the group ring RG to R defined by

$$\sum_{i=1}^{n} a_i g_i \mapsto \sum_{i=1}^{n} a_i$$

is a homomorphism, called the **augmentation map**.
The kernel of the augmentation map, the **augmentation ideal**, is the set of elements of RG whose coefficients sum to 0.
E.g., $g_i - g_j$ is an element of the augmentation ideal for all i, j.
Since the augmentation map is surjective, the quotient ring is isomorphic to R.
Another ideal in RG is $\{\sum_{i=1}^{n} a g_i : a \in R\}$, i.e., the formal sums whose coefficients are all equal (equivalently, all R-multiples of the element $g_1 + \cdots + g_n$).

One-Sided Ideal of a Ring of Matrices

(8) Let R be a commutative ring with identity $1 \neq 0$ and $n \in \mathbb{Z}$, $n \geq 2$. We exhibit some one-sided ideals in the ring $M_n(R)$.

- For each $j \in \{1, 2, \ldots, n\}$, let L_j be the set of all $n \times n$ matrices in $M_n(R)$ with arbitrary entries in the j-th column and zeros in all other columns.
  - It is clear that L_j is closed under subtraction.
  - It follows directly from the definition of matrix multiplication that for any matrix $T \in M_n(R)$ and any $A \in L_j$, the product TA has zero entries in the i-th column, for all $i \neq j$.

  This shows L_j is a left ideal of $M_n(R)$.
- Moreover, L_j is not a right ideal (hence is not a two-sided ideal): To see this, let E_{pq} be the matrix with 1 in the p-th row and q-th column and zeros elsewhere ($p, q \in \{1, \ldots, n\}$). Then $E_{ij} \in L_j$, but $E_{1j}E_{ji} = E_{1i} \notin L_j$ if $i \neq j$. So L_j is not closed under right multiplication by arbitrary ring elements.
- An analogous argument shows that if R_j is the set of all $n \times n$ matrices in $M_n(R)$ with arbitrary entries in the j-th row and zeros in all other rows, then R_j is a right ideal which is not a left ideal.

The Reduction Homomorphism

- The canonical projection map from $\mathbb{Z}$ to $\mathbb{Z}/n\mathbb{Z}$ obtained by factoring out by the ideal $n\mathbb{Z}$ of $\mathbb{Z}$ is referred to as "reducing modulo n".
  Example: Consider the **Diophantine equation** $x^2 + y^2 = 3z^2$ in integers x, y and z. If such integers exist, we may assume x, y and z have no factors in common: Otherwise, we could divide both sides by the square of this common factor to obtain smaller solutions.
  The equation must also hold in any quotient ring and, in particular in $\mathbb{Z}/n\mathbb{Z}$, for any integer n. The choice $n = 4$ is particularly efficacious: The squares mod 4 are just $0^2, 1^2, 2^2, 3^2$, i.e., $0, 1 \pmod 4$. Reading the equation mod 4, we must have $\left\{ \begin{array}{c} 0 \\ 1 \end{array} \right\} + \left\{ \begin{array}{c} 0 \\ 1 \end{array} \right\} \equiv 3 \left\{ \begin{array}{c} 0 \\ 1 \end{array} \right\}$
  $\equiv \left\{ \begin{array}{c} 0 \\ 3 \end{array} \right\} \pmod 4$, where, e.g., $\left\{ \begin{array}{c} 0 \\ 1 \end{array} \right\}$ indicates a choice 0 or 1.
  Checking the few possibilities shows that we must take the 0 each time. Thus, each of x, y and z must be even. This contradicts the assumption of no common factors.

Remaining Isomorphism Theorems

Theorem

Let R be a ring.

(1) (**Second Isomorphism Theorem for Rings**) Let A be a subring and let B be an ideal of R. Then $A + B = \{a + b : a \in A, b \in B\}$ is a subring of R, $A \cap B$ is an ideal of A and $(A + B)/B \cong A/(A \cap B)$.

(2) (**Third Isomorphism Theorem for Rings**) Let I and J be ideals of R with $I \subseteq J$. Then J/I is an ideal of R/I and $(R/I)/(J/I) \cong R/J$.

(3) (**Fourth** or **Lattice Isomorphism Theorem for Rings**) Let I be an ideal of R. The correspondence $A \leftrightarrow A/I$ is an inclusion preserving bijection between the set of subrings A of R that contain I and the set of subrings of R/I. Furthermore, A (a subring containing I) is an ideal of R if and only if A/I is an ideal of R/I.

- We first use the corresponding theorem for groups to obtain an isomorphism of additive groups. Then check that the isomorphism is a multiplicative map, and so defines a ring isomorphism.

Illustration of Proof

- The map that gives the isomorphism in Part (2) is defined by

$$\varphi : r + I \mapsto r + J.$$

This map is multiplicative since

$$\begin{aligned}
\varphi((r_1 + I)(r_2 + I)) &= \varphi(r_1 r_2 + I) \quad \text{(multiplication in } R/I\text{)} \\
&= r_1 r_2 + J \quad \text{(definition of } \varphi\text{)} \\
&= (r_1 + J)(r_2 + J) \quad \text{(multiplication in } R/J\text{)} \\
&= \varphi(r_1 + I)\varphi(r_2 + I). \quad \text{(definition of } \varphi\text{)}
\end{aligned}$$

The proofs for the other parts of are similar.

An Example of the Lattice Isomorphism Theorem

- Let $R = \mathbb{Z}$ and let I be the ideal $12\mathbb{Z}$.
  The quotient ring $\overline{R} = R/I = \mathbb{Z}/12\mathbb{Z}$ has ideals

$$\overline{R},\ 2\mathbb{Z}/12\mathbb{Z},\ 3\mathbb{Z}/12\mathbb{Z},\ 4\mathbb{Z}/12\mathbb{Z},\ 6\mathbb{Z}/12\mathbb{Z},\ \overline{0} = 12\mathbb{Z}/12\mathbb{Z}$$

  corresponding to the ideals

$$R = \mathbb{Z},\ 2\mathbb{Z},\ 3\mathbb{Z},\ 4\mathbb{Z},\ 6\mathbb{Z},\ 12\mathbb{Z} = I$$

  of R containing I, respectively.

Sum and Product of Ideals

Definition (Sum, Product and Power of Ideals)

Let I and J be ideals of R.

(1) Define the **sum** of I and J by $I + J = \{a + b : a \in I, b \in J\}$.

(2) Define the **product** of I and J, denoted by IJ, to be the set of all finite sums of elements of the form ab with $a \in I$ and $b \in J$.

(3) For any $n \geq 1$, define the n-**th power** of I, denoted by I^n, to be the set consisting of all finite sums of elements of the form $a_1 a_2 \cdots a_n$, with $a_i \in I$, for all i.

Equivalently, I^n is defined inductively by defining $I^1 = I$, and $I^n = II^{n-1}$, for $n = 2, 3, \ldots$.

Sum and Product of Ideals

- If I and J are ideals in the ring R, then the set of sums $a + b$ with $a \in I$ and $b \in J$, is not only a subring of R (as in the Second Isomorphism Theorem for Rings), but is an ideal in R:
  - The set is clearly closed under sums;
  - $r(a + b) = ra + rb \in I + J$ since $ra \in I$ and $rb \in J$.
- It is easy to see that:
  - The sum $I + J$ of the ideals I and J is the smallest ideal of R containing both I and J;
  - The product IJ is an ideal contained in $I \cap J$ (but may be strictly smaller).
- Note also that the elements of the product ideal IJ are finite sums of products of elements ab from I and J.

  The set $\{ab : a \in I, b \in J\}$ consisting just of products of elements from I and J is, in general, not closed under addition. Hence, it is not in general an ideal.

Examples

(1) Let $I = 6\mathbb{Z}$ and $J = 10\mathbb{Z}$ in $\mathbb{Z}$.

Then $I + J$ consists of all integers of the form $6x + 10y$ with $x, y \in \mathbb{Z}$. Since every such integer is divisible by 2, the ideal $I + J$ is contained in $2\mathbb{Z}$. On the other hand, $2 = 6(2) + 10(-1)$. Thus, the ideal $I + J$ contains the ideal $2\mathbb{Z}$. So $6\mathbb{Z} + 10\mathbb{Z} = 2\mathbb{Z}$.

In general, $m\mathbb{Z} + n\mathbb{Z} = d\mathbb{Z}$, where d is the greatest common divisor of m and n.

The product IJ consists of all finite sums of elements of the form $(6x)(10y)$, with $x, y \in \mathbb{Z}$. This clearly gives the ideal $60\mathbb{Z}$.

(2) Let I be the ideal in $\mathbb{Z}[x]$ consisting of the polynomials with integer coefficients whose constant term is even. The two polynomials 2 and x are contained in I. So both $4 = 2 \cdot 2$ and $x^2 = x \cdot x$ are elements of the product ideal $I^2 = II$. So is their sum $x^2 + 4$. We may check, however, that $x^2 + 4$ cannot be written as a single product $p(x)q(x)$ of two elements of I.

Subsection 4

Properties of Ideals

Ideals Generated by Subsets in a Ring

- Let R be a ring with identity $1 \neq 0$.

Definition

Let A be any subset of the ring R.

(1) Let (A) denote the smallest ideal of R containing A, called the **ideal generated by** A.

(2) Let RA denote the set of all finite sums of elements of the form ra with $r \in R$ and $a \in A$, i.e., $RA = \{r_1a_1 + r_2a_2 + \cdots + r_na_n : r_i \in R, a_i \in A, n \in \mathbb{Z}^+\}$ (where the convention is $RA = 0$ if $A = \emptyset$).

Similarly, $AR = \{a_1r_1 + a_2r_2 + \cdots + a_nr_n : r_i \in R, a_i \in A, n \in \mathbb{Z}^+\}$ and $RAR = \{r_1a_1r_1' + r_2a_2r_2' + \cdots + r_na_nr_n' : r_i, r_i' \in R, a_i \in A, n \in \mathbb{Z}^+\}$.

(3) An ideal generated by a single element is called a **principal ideal**.

(4) An ideal generated by a finite set is called a **finitely generated ideal**.

- When $A = \{a\}$ or $\{a_1, a_2, \ldots\}$, etc., we shall drop the set brackets and simply write (a), $(a_1, a_2, \ldots)$ for (A), respectively.

RA is Left Ideal Generated by A

- Since the intersection of any nonempty collection of ideals of R is also an ideal, and A is always contained in at least one ideal (namely R), we have $(A) = \bigcap_{\substack{I \text{ an ideal} \\ A \subseteq I}} I$, i.e., (A) is the intersection of all ideals of R that contain the set A.
- The **left ideal generated by** A is the intersection of all left ideals of R that contain A. This left ideal is obtained from A by closing A under all the operations that define a left ideal.
  - It is immediate from the definition that RA is closed under addition and under left multiplication by any ring element. Since R has an identity, RA contains A. Thus RA is a left ideal of R which contains A.
  - Conversely, any left ideal which contains A must contain all finite sums of elements of the form ra, $r \in R$ and $a \in A$ and so must contain RA.

  Thus, RA is precisely the left ideal generated by A.

More Remarks on Ideals

- Similarly, AR is the right ideal generated by A and RAR is the (two-sided) ideal generated by A.
- In particular, if R is commutative then $RA = AR = RAR = (A)$.
- When R is a commutative ring and $a \in R$, the principal ideal (a) generated by a is just the set of all R-multiples of a.
- If R is not commutative the set $\{ras : r, s \in R\}$ is not necessarily the two-sided ideal generated by a, since it need not be closed under addition; In this case the ideal generated by a is the ideal RaR, which consists of all finite sums of elements of the form ras, $r, s \in R$.
- The element $b \in R$ belongs to the ideal (a):
  - if and only if $b = ra$, for some $r \in R$;
  - if and only if b is a **multiple** of a;
  - if and only if a **divides** b in R;
  - if and only if $(b) \subseteq (a)$.

  Thus, containment relations between ideals is seen to capture some of the arithmetic of general commutative rings.

Ideals in $\mathbb{Z}$

(1) The trivial ideal 0 and the ideal R are both principal: $0 = (0)$ and $R = (1)$.

(2) In $\mathbb{Z}$ we have $n\mathbb{Z} = \mathbb{Z}n = (n) = (-n)$, for all integers n. Thus, the notation for aR is consistent with the definition of $n\mathbb{Z}$.

These are all the ideals of $\mathbb{Z}$, so every ideal of $\mathbb{Z}$ is principal.

For positive integers n and m, $n\mathbb{Z} \subseteq m\mathbb{Z}$ if and only if m divides n in $\mathbb{Z}$, so the lattice of ideals containing $n\mathbb{Z}$ is the same as the lattice of divisors of n.

Furthermore, the ideal generated by two nonzero integers n and m is the principal ideal generated by their greatest common divisor, d: $(n, m) = (d)$. The notation for (n, m) as the greatest common divisor of n and m is thus consistent with the same notation for the ideal generated by n and m. In particular, n and m are relatively prime if and only if $(n, m) = (1)$.

Ideals in $\mathbb{Z}[x]$

(3) The ideal $(2, x)$ generated by 2 and x in $\mathbb{Z}[x]$ is not a principal ideal. Observe that $(2, x) = \{2p(x) + xq(x) : p(x), q(x) \in \mathbb{Z}[x]\}$. So this ideal consists precisely of the polynomials with integer coefficients whose constant term is even. In particular, this is a proper ideal. Assume, by way of contradiction, that $(2, x) = (a(x))$, for some $a(x) \in \mathbb{Z}[x]$. Since $2 \in (a(x))$, there must be some $p(x)$, such that $2 = p(x)a(x)$. The degree of $p(x)a(x)$ equals degree$p(x)$+ degree$a(x)$. Hence both $p(x)$ and $a(x)$ must be constant polynomials, i.e., integers. Since 2 is a prime number, $a(x), p(x) \in \{\pm 1, \pm 2\}$.

- If $a(x)$ were ± 1, then every polynomial would be a multiple of $a(x)$, contrary to $(a(x))$ being a proper ideal.
- The only possibility is $a(x) = \pm 2$. But now $x \in (a(x)) = (2) = (-2)$. So $x = 2q(x)$, for some polynomial $q(x)$, with integer coefficients. This is clearly impossible.

This contradiction proves that $(2, x)$ is not principal.

- Later, we show that for any field F, all ideals of $F[x]$ are principal.

Rings of Functions and Group Rings

(4) If R is the ring of all functions from the closed interval $[0,1]$ into $\mathbb{R}$, let M be the ideal $\{f : f(\frac{1}{2}) = 0\}$ (the kernel of evaluation at $\frac{1}{2}$). Let $g(x)$ be the function which is zero at $x = \frac{1}{2}$ and 1 at all other points. Then $f = fg$, for all $f \in M$. So M is a principal ideal with generator g. In fact, any function which is zero at $\frac{1}{2}$ and nonzero at all other points is another generator for the same ideal M.

On the other hand, if R is the ring of all continuous functions from $[0,1]$ to $\mathbb{R}$ then $\{f : f(\frac{1}{2}) = 0\}$ is not principal nor is it even finitely generated.

(5) If G is a finite group and R is a commutative ring with 1, then the augmentation ideal is generated by the set $\{g - 1 : g \in G\}$, although this need not be a minimal set of generators.

For example, if G is a cyclic group with generator σ, then the augmentation ideal is a principal ideal with generator $\sigma - 1$.

Ideals and Units

Proposition

Let I be an ideal of R.

(1) $I = R$ if and only if I contains a unit.

(2) Assume R is commutative. Then R is a field if and only if its only ideals are 0 and R.

(1) If $I = R$, then I contains the unit 1. Conversely, if u is a unit in I with inverse v, then for any $r \in R$, $r = r \cdot 1 = r(vu) = (rv)u \in I$. Hence, $R = I$.

(2) The ring R is a field if and only if every nonzero element is a unit. If R is a field, every nonzero ideal contains a unit. So, by the first part, R is the only nonzero ideal.
Conversely, if 0 and R are the only ideals of R, let u be any nonzero element of R. By hypothesis $(u) = R$. So $1 \in (u)$. Thus, there is some $v \in R$, such that $1 = vu$, i.e., u is a unit. Every nonzero element of R is therefore a unit and so R is a field.

Ideals and Ring Homomorphisms

Corollary

If R is a field then any nonzero ring homomorphism from R into another ring is an injection.

- The kernel of a ring homomorphism is an ideal. The kernel of a nonzero homomorphism is a proper ideal. By the proposition, it is 0.
- If D is a ring with identity $1 \neq 0$ in which the only left ideals and the only right ideals are 0 and D, then D is a division ring.
  Conversely, the only ideals in a division ring D are 0 and D.
  This gives an analog of the proposition if R is not commutative.
- If F is a field, then for any $n \geq 2$, the only two-sided ideals in the matrix ring $M_n(F)$ are 0 and $M_n(F)$, even though this is not a division ring.
  Thus, the proposition does not hold for noncommutative rings.
- Rings whose only two-sided ideals are 0 and the whole ring are called **simple rings**.

Maximal Ideals

Definition (Maximal Ideal)

An ideal M in an arbitrary ring S is called a **maximal ideal** if $M \neq S$ and the only ideals containing M are M and S.

- A general ring need not have maximal ideals:

  E.g., take any abelian group which has no maximal subgroups (say, $\mathbb{Q}$) and make it into a trivial ring by defining $ab = 0$, for all a, b.

  In such a ring the ideals are simply the subgroups and so there are no maximal ideals.

- The zero ring has no maximal ideals.

  Thus, any result involving maximal ideals forces a ring to be nonzero.

Existence of Maximal Ideals in Rings with Identity

Proposition

In a ring with identity every proper ideal is contained in a maximal ideal.

- Let R be a ring with identity and let I be a proper ideal (so R cannot be the zero ring, i.e., $1 \neq 0$). Let $\mathcal{S}$ be the set of all proper ideals of R which contain I. Then S is nonempty ($I \in \mathcal{S}$) and is partially ordered by inclusion. If $\mathcal{C}$ is a chain in $\mathcal{S}$, define J to be the union of all ideals in $\mathcal{C}$: $J = \bigcup_{A \in \mathcal{C}} A$. We first show that J is an ideal:
  - Certainly J is nonempty because $\mathcal{C}$ is nonempty; Specifically, $0 \in J$, since 0 is in every ideal A.
  - If $a, b \in J$, then there are ideals $A, B \in \mathcal{C}$, such that $a \in A$ and $b \in B$. By definition of a chain, either $A \subseteq B$ or $B \subseteq A$. In either case $a - b \in J$, so J is closed under subtraction.
  - Since each $A \in \mathcal{C}$ is closed under left and right multiplication by elements of R, so is J.

  This proves J is an ideal.

Existence of Maximal Ideals (Cont'd)

- If J is not a proper ideal then $1 \in J$.

  In this case, by definition of J, $1 \in A$, for some $A \in \mathcal{C}$.

  This is a contradiction because each A is a proper ideal ($A \in \mathcal{C} \subseteq \mathcal{S}$).

  This proves that each chain has an upper bound in $\mathcal{S}$.

  By Zorn's Lemma, $\mathcal{S}$ has a maximal element.

  That maximal element is a maximal (proper) ideal containing I.

Maximal Ideals in Commutative Rings

- For commutative rings a characterization of maximal ideals by the structure of their quotient ring follows:

Proposition

Assume R is commutative. The ideal M is a maximal ideal if and only if the quotient ring R/M is a field.

- The ideal M is maximal if and only if there are no ideals I with $M \subset I \subset R$. By the Lattice Isomorphism Theorem, the ideals of R containing M correspond bijectively with the ideals of R/M. So M is maximal if and only if the only ideals of R/M are 0 and R/M. By a previous proposition, we see that M is maximal if and only if R/M is a field.
- The proposition above indicates how to construct some fields:

  Take the quotient of any commutative ring R with identity by a maximal ideal in R.

Examples I

(1) Let n be a nonnegative integer. The ideal $n\mathbb{Z}$ of $\mathbb{Z}$ is a maximal ideal if and only if $\mathbb{Z}/n\mathbb{Z}$ is a field. This is the case if and only if n is a prime number.

This also follows directly from the containment of ideals of $\mathbb{Z}$, described previously.

(2) The ideal $(2, x)$ is a maximal ideal in $\mathbb{Z}[x]$ because its quotient ring is the field $\mathbb{Z}/2\mathbb{Z}$.

(3) The ideal (x) in $\mathbb{Z}[x]$ is not maximal since $(x) \subset (2, x) \subset \mathbb{Z}[x]$.

The quotient ring $\mathbb{Z}[x]/(x)$ is isomorphic to $\mathbb{Z}$:

The ideal (x) in $\mathbb{Z}[x]$ is the kernel of the surjective ring homomorphism from $\mathbb{Z}[x]$ to $\mathbb{Z}$, given by evaluation at 0.

$\mathbb{Z}$ not being a field, (x) is not a maximal ideal in $\mathbb{Z}[x]$.

Examples II

(4) Let R be the ring of all functions from $[0,1]$ to $\mathbb{R}$ and for each $a \in [0,1]$, let M_a be the kernel of evaluation at a. Since evaluation is a surjective homomorphism from R to $\mathbb{R}$, we see that $R/M_a \cong \mathbb{R}$. Hence M_a is a maximal ideal.

Similarly, the kernel of evaluation at any fixed point is a maximal ideal in the ring of continuous real valued functions on $[0,1]$.

(5) If F is a field and G is a finite group, then the augmentation ideal I is a maximal ideal of the group ring FG. The augmentation ideal is the kernel of the augmentation map which is a surjective homomorphism onto the field F (i.e., $FG/I \cong F$ a field).

Note that Proposition 12 does not apply directly since FG need not be commutative. However, the implication in Proposition 12 that I is a maximal ideal if R/I is a field holds for arbitrary rings.

Prime Ideals

Definition (Prime Ideal)

Assume R is commutative. An ideal P is called a **prime ideal** if $P \neq R$ and whenever the product ab of two elements $a, b \in R$ is an element of P, then at least one of a and b is an element of P.

- The notion of prime ideal is a natural generalization of the notion of a "prime" in the integers $\mathbb{Z}$.
  Let n be a nonnegative integer. According to the above definition the ideal $n\mathbb{Z}$ is a prime ideal provided:
  - $n \neq 1$ (to ensure that the ideal is proper) and
  - if the product ab of two integers is an element of $n\mathbb{Z}$, at least one of a, b is an element of $n\mathbb{Z}$.
    Put another way, if $n \neq 0$, it must have the property that whenever n divides ab, n must divide a or divide b.

  This is equivalent to the usual definition that n is a prime number.
  Thus the prime ideals of $\mathbb{Z}$ are just the ideals $p\mathbb{Z}$ of $\mathbb{Z}$ generated by prime numbers p together with the ideal 0.

Prime Ideals and Integral Domains

- Recall that an integral domain is a commutative ring with identity $1 \neq 0$ that has no zero divisors.

Proposition

Assume R is commutative. Then the ideal P is a prime ideal in R if and only if the quotient ring R/P is an integral domain.

- The ideal P is prime if and only if $P \neq R$ and whenever $ab \in P$, then either $a \in P$ or $b \in P$. Note that $r \in P$ if and only if $\overline{r} = r + P$ is zero in R/P. Thus, P is a prime ideal if and only if $\overline{R} \neq \overline{0}$ and whenever $\overline{ab} = \overline{a}\overline{b} = \overline{0}$, then either $\overline{a} = \overline{0}$ or $\overline{b} = \overline{0}$, i.e., R/P is an integral domain.
- In particular, a commutative ring with identity is an integral domain if and only if 0 is a prime ideal.

Relation Between Maximal and Prime Ideals

Corollary

Assume R is commutative. Every maximal ideal of R is a prime ideal.

- If M is a maximal ideal then R/M is a field. A field is an integral domain. So M is prime.

  Examples:

  (1) The principal ideals generated by primes in $\mathbb{Z}$ are both prime and maximal ideals.
  The zero ideal in $\mathbb{Z}$ is prime but not maximal.

  (2) The ideal (x) is a prime ideal in $\mathbb{Z}[x]$ since $\mathbb{Z}[x]/(x) \cong \mathbb{Z}$. This ideal is not a maximal ideal.
  The ideal 0 is a prime ideal in $\mathbb{Z}[x]$, but is not a maximal ideal.

Subsection 5

Rings of Fractions

Non-zero Divisors and Invertibility

- We deal with a commutative ring R.
  - We know that if a is not zero nor a zero divisor and $ab = ac$ in R then $b = c$. Thus, a nonzero element that is not a zero divisor enjoys some of the properties of a unit without necessarily possessing a multiplicative inverse in R.
  - On the other hand, a zero divisor a cannot be a unit in R and, by definition, if a is a zero divisor, we cannot always cancel the a's in the equation $ab = ac$ to obtain $b = c$ (take $c = 0$, for example).
- We prove that a commutative ring R is always a subring of a larger ring Q in which every nonzero element of R that is not a zero divisor is a unit in Q.
- The principal application of this will be to integral domains, in which case this ring Q will be a field - called its **field of fractions** or **quotient field**.
- The paradigm for the construction of Q from R is the construction of the field of rational numbers from the integral domain $\mathbb{Z}$.

Construction of $\mathbb{Q}$ from $\mathbb{Z}$

- Each rational number may be represented in many different ways as the quotient of two integers (e.g., $\frac{1}{2} = \frac{2}{4} = \frac{3}{6} = \cdots$).
  These representations are related by $\frac{a}{b} = \frac{c}{d}$ iff $ad = bc$.
- The fraction b is the equivalence class of ordered pairs (a, b) of integers with $b \neq 0$ under the equivalence relation $(a, b) \sim (c, d)$ if and only if $ad = bc$.
- The arithmetic operations on fractions are given by

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} \quad \text{and} \quad \frac{a}{b} \times \frac{c}{d} = \frac{ac}{bd}.$$

  These are well defined (independent of choice of representatives of the equivalence classes).
- They make the set of fractions into a commutative ring (in fact, a field), $\mathbb{Q}$.
- The integers $\mathbb{Z}$ are identified with the subring $\{\frac{a}{1} : a \in \mathbb{Z}\}$ of $\mathbb{Q}$.
- Every nonzero integer a has an inverse $\frac{1}{a}$ in $\mathbb{Q}$.

Problems Involving Zero Divisors

- Suppose R is any commutative ring and we allow arbitrary denominators.
- If b is zero or a zero divisor in R, say $bd = 0$, and we allow b as a denominator, then, assuming R has a 1, in the "ring of fractions", we would have $d = \frac{d}{1} = \frac{bd}{b} = \frac{0}{b} = 0$.

  Thus, if we allow zero or zero divisors as denominators, there must be some collapsing in the sense that we cannot expect R to appear naturally as a subring of this "ring of fractions".
- A second restriction is more obviously imposed by the laws of addition and multiplication:

  If ring elements b and d are allowed as denominators, then bd must also be a denominator. Hence, the set of denominators must be closed under multiplication in R.
- These two restrictions are sufficient to construct a ring of fractions for R, which includes the construction of $\mathbb{Q}$ from $\mathbb{Z}$ as a special case.

The Ring of Fractions Theorem

Theorem

Let R be a commutative ring. Let D be any nonempty subset of R that does not contain 0, does not contain any zero divisors and is closed under multiplication (i.e., $ab \in D$, for all $a, b \in D$). Then there is a commutative ring Q with 1, such that Q contains R as a subring and every element of D is a unit in Q. The ring Q has the following additional properties:

(1) Every element of Q is of the form rd^{-1}, for some $r \in R$ and $d \in D$. In particular, if $D = R - \{0\}$, then Q is a field.

(2) (Uniqueness of Q) The ring Q is the "smallest" ring containing R in which all elements of D become units, in the following sense:

Let S be any commutative ring with identity and let $\varphi : R \to S$ be any injective ring homomorphism such that $\varphi(d)$ is a unit in S, for every $d \in D$. Then there is an injective homomorphism $\Phi : Q \to S$, such that $\Phi|_R = \varphi$. In other words, any ring containing an isomorphic copy of R in which all the elements of D become units must also contain an isomorphic copy of Q.

Proof of the Theorem: The Construction

- Let $\mathcal{F} = \{(r, d) : r \in R, d \in D\}$ and define the relation $\sim$ on $\mathcal{F}$ by $(r, d) \sim (s, e)$ if and only if $re = sd$. This relation is reflexive and symmetric. Suppose $(r, d) \sim (s, e)$ and $(s, e) \sim (t, f)$. Then $re - sd = 0$ and $sf - te = 0$. Multiply the first by f and the second by d and add: $(rf - td)e = 0$. Since $e \in D$ is neither zero nor a zero divisor, we must have $rf - td = 0$, i.e., $(r, d) \sim (t, f)$. This proves $\sim$ is transitive. Hence, $\sim$ is an equivalence relation. Denote the equivalence class of (r, d) by $\frac{r}{d}$:

$$\frac{r}{d} = \{(a, b) : a \in R, b \in D \text{ and } rb = ad\}.$$

Let Q be the set of $\sim$-equivalence classes. Note that $\frac{r}{d} = \frac{re}{de}$, for all $e \in D$, since D is closed under multiplication.

Define an additive and multiplicative structure on Q:

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} \quad \text{and} \quad \frac{a}{b} \times \frac{c}{d} = \frac{ac}{bd}.$$

Proof of the Theorem: The Desiderata

- We defined

$$\frac{a}{b}+\frac{c}{d}=\frac{ad+bc}{bd} \quad \text{and} \quad \frac{a}{b}\times\frac{c}{d}=\frac{ac}{bd}.$$

In order to prove that Q is a commutative ring with identity there are a number of things to check:

(1) These operations are well defined (i.e., do not depend on the choice of representatives for the equivalence classes);
(2) Q is an abelian group under addition, where the additive identity is $\frac{0}{d}$, for any $d \in D$, and the additive inverse of $\frac{a}{d}$ is $\frac{-a}{d}$;
(3) Multiplication is associative, distributive and commutative;
(4) Q has an identity ($= \frac{d}{d}$, for any $d \in D$).

These are all straightforward calculations involving only arithmetic in R and the definition of $\sim$.

We need D to be closed under multiplication for addition and multiplication to be defined.

Proof of the Theorem: Properties

- We check that addition is well defined:

  Assume $\frac{a}{b} = \frac{a'}{b'}$, i.e., $ab' = a'b$, and $\frac{c}{d} = \frac{c'}{d'}$, i.e., $cd' = c'd$.
  We must show that

  $$\frac{ad + bc}{bd} = \frac{a'd' + b'c'}{b'd'},$$

  i.e., $(ad + bc)(b'd') = (a'd' + b'c')(bd)$.

  - The left hand side of this equation is $ab'dd' + cd'bb'$.
  - Substituting $a'b$ for ab' and $c'd$ for cd' gives $a'bdd' + c'dbb'$.
  - This is the right hand side.

  Hence addition of fractions is well defined.

Checking the details in the other parts of (1) to (4) involves easier manipulations.

Proof of the Theorem: Embedding R in Q

- Next we embed R into Q by defining $\iota : R \to Q$ by $\iota : r \mapsto \frac{rd}{d}$, where d is any element of D. Since $\frac{rd}{d} = \frac{re}{e}$, for all $d, e \in D$, $\iota(r)$ does not depend on the choice of $d \in D$.
  - Since D is closed under multiplication, one checks directly that ι is a ring homomorphism.
  - Furthermore, ι is injective because $\iota(r) = 0 \Leftrightarrow \frac{rd}{d} = \frac{0}{d} \Leftrightarrow rd^2 = 0 \Leftrightarrow r = 0$ because d (hence also d^2) is neither zero nor a zero divisor.

  The subring $\iota(R)$ of Q is therefore isomorphic to R.
- We henceforth identify each $r \in R$ with $\iota(r)$ and so consider R as a subring of Q.
- Each $d \in D$ has a multiplicative inverse in Q: If d is represented by the fraction $\frac{de}{e}$, then its multiplicative inverse is $\frac{e}{de}$.
- One then sees that every element of Q may be written as $r \cdot d^{-1}$, for some $r \in R$ and some $d \in D$. In particular, if $D = R - \{0\}$, every nonzero element of Q has a multiplicative inverse and Q is a field.

Proof of the Theorem: Uniqueness

- To establish the uniqueness property of Q, assume $\varphi : R \to S$ is an injective ring homomorphism such that $\varphi(d)$ is a unit in S, for all $d \in D$. Extend φ to a map $\Phi : Q \to S$ by defining

$$\Phi(rd^{-1}) = \varphi(r)\varphi(d)^{-1}, \quad \text{for all } r \in R, d \in D.$$

Φ is well defined: $rd^{-1} = se^{-1} \Rightarrow re = sd \Rightarrow \varphi(r)\varphi(e) = \varphi(s)\varphi(d)$ $\Rightarrow \Phi(rd^{-1}) = \varphi(r)\varphi(d)^{-1} = \varphi(s)\varphi(e)^{-1} = \Phi(se^{-1})$.

  - It is straightforward to check that Φ is a ring homomorphism.
  - Φ is injective: $rd^{-1} \in \ker\Phi$ implies $r \in \ker\Phi \cap R = \ker\varphi$. Since φ is injective this forces $r = 0$ and, hence $rd^{-1} = 0$.

Definition (Ring of Fractions and Field of Fractions)

Let R, D and Q be as in the theorem.

(1) The ring Q is called the **ring of fractions** of D with respect to R and is denoted $D^{-1}R$.

(2) If R is an integral domain and $D = R - \{0\}$, Q is called the **field of fractions** or **quotient field** of R.

Subfields Generated By Subsets

- If A is a subset of a field F (for example, if A is a subring of F), then the intersection of all the subfields of F containing A is a subfield of F.
- It is called the **subfield generated** by A.
- This subfield is the smallest subfield of F containing A:

  Any subfield of F containing A contains the subfield generated by A.

Subfield Generated by a Ring and Field of Fractions

Corollary

Let R be an integral domain and let Q be the field of fractions of R. If a field F contains a subring R' isomorphic to R, then the subfield of F generated by R' is isomorphic to Q.

- Let $\varphi : R \to R' \subseteq F$ be a (ring) isomorphism of R to R'. In particular, $\varphi : R \to F$ is an injective homomorphism from R into the field F. Let $\Phi : Q \to F$ be the extension of φ to Q. By the theorem, Φ injective. So $\Phi(Q)$ is an isomorphic copy of Q in F containing $\varphi(R) = R'$. Now, any subfield of F containing $R' = \varphi(R)$ contains the elements $\varphi(r_1)\varphi(r_2)^{-1} = \varphi(r_1 r_2^{-1})$, for all $r_1, r_2 \in R$. But every element of Q is of the form $r_1 r_2^{-1}$, for some $r_1, r_2 \in R$. Thus, any subfield of F containing R' contains the field $\Phi(Q)$. So $\Phi(Q)$ is the subfield of F generated by R'.

Examples

(1) If R is a field then its field of fractions is just R itself.

(2) The integers $\mathbb{Z}$ are an integral domain whose field of fractions is the field $\mathbb{Q}$ of rational numbers.

The quadratic integer ring $\mathbb{Z}(\sqrt{D})$ is an integral domain whose field of fractions is the quadratic field $\mathbb{Q}(\sqrt{D})$.

(3) The subring $2\mathbb{Z}$ of $\mathbb{Z}$ also has no zero divisors (but has no identity). Its field of fractions is also $\mathbb{Q}$.

The Field of Rational Functions

(4) If R is any integral domain, then the polynomial ring $R[x]$ is also an integral domain. The associated field of fractions is the field of **rational functions** in the variable x over R.

The elements of this field are of the form $\frac{p(x)}{q(x)}$, where $p(x)$ and $q(x)$ are polynomials with coefficients in R with $q(x)$ not the zero polynomial. In particular, $p(x)$ and $q(x)$ may both be constant polynomials, so the field of rational functions contains the field of fractions of R: elements of the form $\frac{a}{b}$, such that $a, b \in R$ and $b \neq 0$.

If F is a field, we shall denote the field of rational functions by $F(x)$. Thus, if F is the field of fractions of the integral domain R, then the field of rational functions over R is the same as the field of rational functions over F, namely $F(x)$.

Fields of Rational Functions of $\mathbb{Q}[x]$ and $\mathbb{Z}[x]$

- Example: Suppose $R = \mathbb{Z}$, so $F = \mathbb{Q}$. If $p(x), q(x)$ are polynomials in $\mathbb{Q}[x]$, then for some integer N, $Np(x), Nq(x)$ have integer coefficients (e.g., let N be a common denominator for all the coefficients in $p(x)$ and $q(x)$). Then

$$\frac{p(x)}{q(x)} = \frac{Np(x)}{Nq(x)}$$

can be written as the quotient of two po1ynomials with integer coefficients. So the field of fractions of $\mathbb{Q}[x]$ is the same as the field of fractions of $\mathbb{Z}[x]$.

The Ring $R[1/d]$

(5) Let R is any commutative ring with identity.

Let d be neither zero nor a zero divisor in R.

Form the ring $R[1/d]$ by setting:

- $D = \{1, d, d^2, d^3, \ldots\}$;
- $R[1/d]$ be the ring of fractions $D^{-1}R$.

Note that R is the subring of elements of the form $\frac{r}{1}$.

In this way any nonzero element of R that is not a zero divisor can be inverted in a larger ring containing R.

Note that the elements of $R[1/d]$ look like polynomials in $\frac{1}{d}$, with coefficients in R, which explains the notation.

Subsection 6

The Chinese Remainder Theorem

Ring Direct Products

- We assume that all rings are commutative with an identity $1 \neq 0$.
- Given an arbitrary collection of rings (not necessarily satisfying the conventions above), their (**ring**) **direct product** is defined to be their direct product as (abelian) groups made into a ring by defining multiplication componentwise.
- In particular, if R_1 and R_2 are two rings, we shall denote by $R_1 \times R_2$ their direct product (as rings).

  This is, the set of ordered pairs (r_1, r_2), with $r_1 \in R_1$ and $r_2 \in R_2$, where addition and multiplication are performed componentwise:

  $$(r_1, r_2)+(s_1, s_2) = (r_1+s_1, r_2+s_2) \quad \text{and} \quad (r_1, r_2)(s_1, s_2) = (r_t s_1, r_2 s_2).$$

- A map φ from a ring R into a direct product ring is a homomorphism if and only if the induced maps into each of the components are homomorphisms.

Comaximal Ideals

- There is a generalization to arbitrary rings of the notion in $\mathbb{Z}$ of two integers n and m being relatively prime.
- In $\mathbb{Z}$ this is equivalent to being able to solve the equation $nx + my = 1$ in integers x and y. This in turn is equivalent to $n\mathbb{Z} + m\mathbb{Z} = \mathbb{Z}$ as ideals (in general, $n\mathbb{Z} + m\mathbb{Z} = (m, n)\mathbb{Z}$).

Definition (Comaximal Ideals)

The ideals A and B of the ring R are said to be **comaximal** if $A + B = R$.

- Recall that the *product* AB, of the ideals A, B of R is the ideal consisting of all finite sums of elements xy, $x \in A$ and $y \in B$.

  If $A = (a)$ and $B = (b)$, then $AB = (ab)$.
- More generally, the **product** of the ideals $A_1, A_2, \ldots, A_k$ is the ideal of all finite sums of elements $x_1 x_2 \cdots x_k$, such that $x_i \in A_i$, for all i.

  If $A_i = (a_i)$, then $A_1 \cdots A_k = (a_1 \cdots a_k)$.

The Chinese Remainder Theorem

Theorem (Chinese Remainder Theorem)

Let $A_1, A_2, \ldots, A_k$ be ideals in R. The map

$$R \mapsto R/A_1 \times R/A_2 \times \cdots \times R/A_k;\ r \mapsto (r + A_1, r + A_2, \ldots, r + A_k)$$

is a ring homomorphism with kernel $A_1 \cap A_2 \cap \cdots \cap A_k$.
If, for each $i, j \in \{1, 2, \ldots, k\}$, with $i \neq j$, the ideals A_i and A_j are comaximal, then this map is surjective and

$$A_1 \cap A_2 \cap \cdots \cap A_k = A_1 A_2 \cdots A_k.$$

So

$$\begin{aligned} R/(A_1 A_2 \cdots A_k) &= R/(A_1 \cap A_2 \cap \cdots \cap A_k) \\ &\cong R/A_1 \times R/A_2 \times \cdots \times R/A_k. \end{aligned}$$

The Chinese Remainder Theorem ($k = 2$)

- We first prove this for $k = 2$. The general case follows by induction.

  Let $A = A_1$ and $B = A_2$. Consider the map $\varphi : R \to R/A \times R/B$ defined by

  $$\varphi(r) = (r \mod A, r \mod B),$$

  where mod A means the class in R/A containing r (that is, $r + A$).

  This map is a ring homomorphism because φ is just the natural projection of R into R/A and R/B for the two components.

  The kernel of φ consists of all the elements $r \in R$ that are in A and in B, i.e., $A \cap B$.

  To complete the proof in this case it remains to show that when A and B are comaximal, φ is surjective and

  $$A \cap B = AB.$$

The Chinese Remainder Theorem (Cont'd)

- φ is surjective: Since $A + B = R$, there are elements $x \in A$ and $y \in B$, such that $x + y = 1$. This equation shows that $\varphi(x) = (0, 1)$ and $\varphi(y) = (1, 0)$ since, e.g., x is an element of A and $x = 1 - y \in 1 + B$. Suppose $(r_1 \mod A, r_2 \mod B)$ is arbitrary in $R/A \times R/B$. Then the element $r_2x + r_1y$ maps to this element:

$$\begin{aligned} \varphi(r_2x + r_1y) &= \varphi(r_2)\varphi(x) + \varphi(r_1)\varphi(y) \\ &= (r_2 \mod A, r_2 \mod B)(0, 1) \\ &\qquad + (r_1 \mod A, r_1 \mod B)(1, 0) \\ &= (0, r_2 \mod B) + (r_1 \mod A, 0) \\ &= (r_1 \mod A, r_2 \mod B). \end{aligned}$$

  This shows that φ is indeed surjective.
- Finally, the ideal AB is always contained in $A \cap B$. Suppose A and B are comaximal. Let x and y be as above. Then, for any $c \in A \cap B$, $c = c1 = cx + cy \in AB$. Thus, $A \cap B \subseteq AB$. Therefore, $A \cap B = AB$.

The proof for $k = 2$ is complete.

The Chinese Remainder Theorem (Induction Step)

- The general case follows easily by induction from the case of two ideals using $A = A_1$ and $B = A_2 \cdots A_k$ once we show that A_1 and $A_2 \cdots A_k$ are comaximal.

  By hypothesis, for each $i \in \{2, 3, \ldots, k\}$, there are elements $x_i \in A_1$ and $y_i \in A_i$, such that

  $$x_i + y_i = 1.$$

  But $x_i + y_i = y_i \mod A_1$.

  Hence

  $$1 = (x_2 + y_2) \cdots (x_k + y_k) \in A_1 + (A_2 \cdots A_k).$$

  Thus, A and B are indeed comaximal.

The Special Case of $\mathbb{Z}/mn\mathbb{Z}$

- The theorem obtained its name from the special case

$$\mathbb{Z}/mn\mathbb{Z} \cong (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z})$$

  as rings when m and n are relatively prime integers.
- This isomorphism relates to simultaneously solving two congruences modulo relatively prime integers:
  It states that such congruences can always be solved, and uniquely.
- Since the isomorphism in the Chinese Remainder Theorem is an isomorphism of rings, in particular the groups of units on both sides must be isomorphic.
  It is easy to see that the units in any direct product of rings are the elements that have units in each of the coordinates.
  In the case of $\mathbb{Z}/mn\mathbb{Z}$, the Chinese Remainder Theorem gives the following isomorphism on the groups of units:

$$(\mathbb{Z}/mn\mathbb{Z})^\times \cong (\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times.$$

The Case for $\mathbb{Z}/n\mathbb{Z}$

Corollary

Let n be a positive integer and let $p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ be its factorization into powers of distinct primes. Then, as rings,

$$\mathbb{Z}/n\mathbb{Z} \cong (\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z}) \times (\mathbb{Z}/p_2^{\alpha_2}\mathbb{Z}) \times \cdots \times (\mathbb{Z}/p_k^{\alpha_k}\mathbb{Z}).$$

In particular we have the following isomorphism of multiplicative groups:

$$(\mathbb{Z}/n\mathbb{Z})^\times \cong (\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z})^\times \times (\mathbb{Z}/p_2^{\alpha_2}\mathbb{Z}) \times \cdots \times (\mathbb{Z}/p_k^{\alpha_k}\mathbb{Z}).$$

Multiplicativity of the Euler φ-Function

- Comparing orders on the two sides of the isomorphism

$$(\mathbb{Z}/n\mathbb{Z})^\times \cong (\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z})^\times \times (\mathbb{Z}/p_2^{\alpha_2}\mathbb{Z}) \times \cdots \times (\mathbb{Z}/p_k^{\alpha_k}\mathbb{Z})$$

  we get, for the Euler φ-function,

$$\varphi(n) = \varphi(p_1^{\alpha_1})\varphi(p_2^{\alpha_2}) \cdots \varphi(p_k^{\alpha_k}).$$

- This implies that φ is a **multiplicative function**, i.e., that $\varphi(ab) = \varphi(a)\varphi(b)$, for a, b relatively prime positive integers.
- The value of φ on prime powers p^α is easily seen to be

$$\varphi(p^\alpha) = p^{\alpha-1}(p-1).$$

- From this and the multiplicativity of φ we obtain its value on all positive integers.