Math 451: Abstract Algebra I

Wolmer V. Vasconcelos

Set 5: Rings

Fall 2009
Outline

1. Rings
2. Integers and Polynomials
3. Homomorphisms
4. Quotient rings and relations in a ring
5. Integral Domains and Rings of Fractions
6. Homework #10
7. Maximal Ideals
8. Noetherian Rings
9. Algebraic Geometry
10. Diagonalization
11. Diagonalization and Minimal Polynomials
12. Homework #11
A ring $R$ is a set with two composition laws, called ‘addition’ and ‘multiplication’, say $+$ and $\times$: $\forall a, b \in R$ have compositions $a + b$ and $a \times b$. (The second composition is also written $a \cdot b$, or simply $ab$.)

- $(R, +)$ is an abelian group
- $(R, \times)$: multiplication is associative, and distributive over $+$, that is $\forall a, b, c \in R$,

\[
(ab)c = a(bc), \quad ab = ba, \quad a(b + c) = ab + ac
\]
• **existence of identity**: \( \exists e \in R \) such that

\[
\forall a \in R \quad e \times a = a \times e = a
\]

• If \( ab = ba \) for all \( a, b \in R \), the ring is called **commutative**

There is a unique identity element \( e \), usually we denote it by 1:

\[
e = ee' = e'e = e'
\]
Some terminology in studying a commutative ring

Let $R$ be a commutative ring

- $u \in R$ is a **unit** if there is $v \in R$ such that $uv = 1$
- $a \in R$ is a **zero divisor** if there is $0 \neq b \in R$ such that $ab = 0$: $\overline{2} \cdot \overline{3} \equiv 0 \text{ in } \mathbb{Z}_6$.
- $a \in R$ is **nilpotent** if there is $n \in \mathbb{N}$ such that $a^n = 0$: $\overline{2}^3 \equiv 0 \text{ in } \mathbb{Z}_8$.
- $R$ is an **integral domain** if 0 is the only zero divisor, in other words, if $a, b \in R$ are not zero, then $ab \neq 0$. 

A field $\mathbf{F}$ is a set with two composition laws, called ‘addition’ and ‘multiplication’, say $+\,$ and $\times:\, \forall a, b \in \mathbf{F}$ have compositions $a + b$ and $a \times b$. (The second composition is also written $a \cdot b$, or simply $ab$.)

- $(\mathbf{F}, +)$ is an abelian group
- $(\mathbf{F}, \times)$: multiplication is associative, commutative and distributive over $+$, that is $\forall a, b, c \in \mathbf{F}$,

\[(ab)c = a(bc), \quad ab = ba, \quad a(b + c) = ab + ac\]
• **existence of identity** \( \exists e \in F \) such that

\[
\forall a \in F \quad a \times e = a
\]

• **existence of inverses** For every \( a \neq 0 \), there is \( b \in F \)

\[
a \times b = e.
\]

There is a unique element \( e \), usually we denote it by 1. For \( a \neq 0 \), the element \( b \) such that \( ab = 1 \) is unique; it is often denoted by \( 1/a \) or \( a^{-1} \).

We can now define **scalars**: the elements of a field.
Fields are ubiquitous:

- $\mathbb{R}$: real numbers

- The integers $\mathbb{Z}$ is not a field (not all integers have inverses), but $\mathbb{Q}$, the rational numbers is a field.

- $\mathbb{C}$: complex numbers, $z = a + bi$, $i = \sqrt{-1}$, with compositions

\[
(a + bi) + (c + di) = (a + c) + (b + d)i
\]

\[
(a + bi) \times (c + di) = (ac - bd) + (ad + bc)i
\]
The arithmetic here requires a bit more care:

If $a + bi \neq 0$,

$$\frac{1}{a + bi} = \frac{a - bi}{a^2 + b^2} = \frac{a}{a^2 + b^2} - \frac{b}{a^2 + b^2}i$$
Exercise: Number fields

Let \( F \) be the set of all real numbers of the form
\[
z = a + b\sqrt{2}, \quad a, b \in \mathbb{Q}
\]
prove that \( F \) is a field.

Query: How to prove a subset \( F \) of the field \( \mathbb{R} \) is a field?
Suffices to check that \( F \) is closed under addition, product and inverse of nonzero element.
For instance, if \( a + b\sqrt{2} \neq 0 \),
\[
\frac{1}{a + b\sqrt{2}} = \frac{a - b\sqrt{2}}{a^2 - 2b^2} \in F
\]
Another noteworthy example is $\mathbb{F}_2$, the set made up by two elements \{0, 1\} (or (even, odd)) with addition defined by the table

\[
\begin{array}{c|cc}
+ & 0 & 1 \\
\hline
0 & 0 & 1 \\
1 & 1 & 0 \\
\end{array}
\]

$1 + 1 = 0!$

and multiplication by

\[
\begin{array}{c|cc}
\times & 0 & 1 \\
\hline
0 & 0 & 0 \\
1 & 0 & 1 \\
\end{array}
\]
Exercise 1: Prove that in any field $F$ the rule minus times minus is plus holds, that is for any $a, b \in F$,

$$-(-a) = a, \quad (-a)(-b) = ab.$$  

Solution: The first assertion follows from

$$a + (-a) = (-a) + a = O.$$  

Because of the above, we must show that $(-a)(-b)$ is the negative of $-(ab)$. We first claim $(-a)b = -(ab)$. Note

$$( -a ) b + a b = ( ( -a ) + a ) b = Ob = O.$$  

$$( -a ) ( -b ) - ( ab ) = ( -a ) ( -b ) + ( -a ) b = ( -a ) ( ( -b ) + b ) = ( -a ) O = O.$$
A field is the mathematical structure of choice to do arithmetic. Given a field $\mathbf{F}$, fractions can defined as follows: If $a, b \in \mathbf{F}, \quad b \neq 0,$

$$\frac{a}{b} := ab^{-1}.$$  

The usual calculus of fractions then follows, for instance

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}.$$
Rings of Functions

Let $\mathbb{R}$ be a ring, $S$ a nonempty set and $S$ the set of all functions $f : S \rightarrow \mathbb{R}$.

**Proposition**

We endow $\mathcal{R}$ with a ring structure by defining two operations:

For all $s \in S$,

$$(f + g)(s) := f(s) + g(s)$$

$$(f \cdot g)(s) := f(s) \cdot g(s)$$

**Proof.** It is clear that $\mathcal{R}$ inherits all the ring axioms from $\mathbb{R}$.  

- If $1 \in \mathbb{R}$, the function $l(s) = 1$ is the identity of $\mathcal{R}$.
- If $\mathbb{R}$ is commutative, $\mathcal{R}$ is also commutative.
- Major examples: If $S = \mathbb{R}$, and $f$ are continuous.
Let $R = M_n(\mathbb{R})$ be the set of all $n \times n$ matrices ($n$ fixed), with the ordinary matrix addition and multiplication.

$R$ is a ring, but it is not \textit{commutative} if $n > 1$. 
Subrings

**Definition**

A subring of a ring $R$ is a subset $S$ that satisfies:

1. $S$ is a subgroup of $R^+$;
2. $1_R \in S$;
3. If $a, b \in S$, then $ab \in S$. (This product is the product of $R$.)

**Example**

$\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ is a tower of rings/subrings. Later, when we have more examples of rings, we will give various methods to construct subrings.
Rational Numbers

At the outset of our journey are the natural numbers

\[ \mathbb{N} = \{1, 2, 3, 4, \ldots\} \]

Its ‘modern’ construction [e.g. Peano’s] is a paradigm of beauty. It is enlarged by the integers

\[ \mathbb{N} \subset \mathbb{Z} = \{\ldots, -4, -3, -2, -1, 0, 1, 2, 3, 4, \ldots\} \]

and the rational numbers

\[ \mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} = \left\{ \frac{m}{n}, \quad m, n \in \mathbb{Z}, n \neq 0 \right\} \]

These sets exhibit different structures: of a monoid, of a ring and of a field, respectively.
The construction by Peano of the set \( \mathbb{N} \) is grounded on two ingredients: The set \( \mathbb{N} \) contains a particular element 1.

- **[Successor Function]** There is a function \( s : \mathbb{N} \to \mathbb{N} \) that is injective, and for every \( n \in \mathbb{N} \) \( s(n) \neq 1 \).
- **[Induction Axiom]** If the subset \( S \subset \mathbb{N} \) has the properties

\[
1 \in S \quad \& \quad \text{whenever} \quad n \in S \Rightarrow s(n) \in S
\]

then \( S = \mathbb{N} \)
Given these definitions, we can define several operations/compositions and structures on \( \mathbb{N} \):

- \( a + b := ? \)

\[
\begin{align*}
    a + 1 & := s(a) \\
    a + s(n) & := s(a + n)
\end{align*}
\]

- \( a \times b := ? \)

\[
\begin{align*}
    a \times 1 & := a \\
    a \times s(n) & := a \times n + a
\end{align*}
\]
Out of these notions, addition and multiplication are defined in $\mathbb{N}$, and then extended to $\mathbb{Z}$ and $\mathbb{Q}$. An interesting consequence that arises is a notion of order: $\forall a, b \in \mathbb{Q}$, exactly one of the following holds:

$$a < b, \quad a > b, \quad a = b$$

It has the properties: If $a > b$ then

$$\forall c \quad \Rightarrow \quad a + c > b + c$$
$$\forall c > 0 \quad \Rightarrow \quad ac > bc$$

**Significance:** This leads to metric properties: lengths, angles, etc.
Peano and Mathematical Induction

http://upload.wikimedia.org/wikipedia/commons/3/3a/Giuseppe_Peano.jpg
Induction

The set $\mathbb{N} = \{1, 2, 3, \ldots\}$ of natural numbers arises logically from the following construction of Peano.

**$\mathbb{Z}$ and Peano’s Axioms**

- $\mathbb{N}$ contains a particular element 1.
- **Successor function:** There is an injective [one-one] function $\sigma : \mathbb{N} \rightarrow \mathbb{N}$, for each $n \in \mathbb{N}$, $\sigma(n) \neq 1$. [Another notation: $\sigma(n) = n'$]
- **Induction axiom:** Suppose that $S \subset \mathbb{N}$ satisfies
  1. $1 \in S$;
  2. If $n \in S$ then $\sigma(n) \in S$. Then $S = \mathbb{N}$.

The second axiom means 3 things [there are 5 axioms in all]:
(1) every natural number has a successor; (2) no two natural numbers have the same successor; (3) 1 is not the successor of any natural number.
Defining Operations $+$ and $\times$

Operations

- **Addition:**
  \[ m + 1 = m', \quad m + n' = (m + n)' \]

- **Multiplication:**
  \[ m \cdot 1 = m, \quad m \cdot n' = m \cdot n + m \]
With these operations, \( \mathbb{N} \) satisfies:

- **Associativity properties:** For all \( x, y \) and \( z \) in \( \mathbb{N} \),
  
  \[
  x + (y + z) = (x + y) + z.
  \]
  
  \[
  x(yz) = (xy)z.
  \]

- **Commutativity properties:** For all \( x \) and \( y \) in \( \mathbb{N} \),
  
  \[
  x + y = y + x.
  \]
  
  \[
  xy = yx.
  \]

- **Distributivity properties:** For all \( x, y \) and \( z \) in \( \mathbb{N} \),
  
  \[
  x(y + z) = xy + xz.
  \]
  
  \[
  (y + z)x = yx + zx.
  \]
Order properties: For all $x, y$ and $z$ in $\mathbb{N}$, $x < y$ if there is $w \in \mathbb{N}$ such that $x + w = y$. Several properties arise: e.g. If $x < y$ then $\forall z \in \mathbb{N} \ x + z < y + z$. 
\( \mathbb{N} \) can extended by 0 and ‘negatives’: \( \mathbb{Z} \). Operations also. Then all the ordinary properties of addition and multiplication are verified:

Let us illustrate with:

**Proof of the associative law of addition for \( \mathbb{N} \):**

\[(a + b) + n = a + (b + n) \quad \forall a, b, n \in \mathbb{N}\]

From the definitions check \( n = 1 \):

\[(a + b) + 1 = (a + b)' = a + b' = a + (b + 1)\]
Assume axiom holds for $n$ and let us check for $n'$ (induction hypothesis):

$$(a + b) + n' = (a + b) + (n + 1) \text{ (definition)}$$

$$= ((a + b) + n) + 1 \text{ (case } n = 1)$$

$$= (a + (b + n)) + 1 \text{ (ind. hypothesis)}$$

$$= a + ((b + n) + 1) \text{ (case } n = 1)$$

$$= a + (b + (n + 1)) \text{ (case } n = 1)$$

$$= a + (b + n') \text{ (definition)}$$
Principle of Mathematical Induction

Let us state Peano’s 5th Axiom again:

**Definition (PMI)**

If $S$ is a subset of $\mathbb{N}$ and

1. $1 \in S$,
2. for all $n \in \mathbb{N}$, if $n \in S$, then $n + 1 \in S$,

then $S = \mathbb{N}$.

A set with Property (2) is called an **inductive set**. Examples, besides $\mathbb{N}$ are $\emptyset$, $S = \{x : x \in \mathbb{N}, x \geq 10\}$. $\mathbb{N}$ is the only inductive set containing 1: This is **PMI**.

The **PMI** is used to define mathematical objects and in proofs galore.
We are discussing the **Principle of Mathematical Induction** (**PMI** for short). It is a mechanism to study (i.e. prove) certain open sentences \( P(n) \) that depend on \( n \in \mathbb{N} \) when we seek to verify that it is true for all values.

The method is rooted in the following property of the **natural numbers** \( \mathbb{N} \):

If \( S \) is a subset of \( \mathbb{N} \) and

1. \( 1 \in S \),
2. for all \( n \in \mathbb{N} \), if \( n \in S \), then \( n + 1 \in S \),

then \( S = \mathbb{N} \).
Verifying $P(n)$

To verify whether $S = \{ n : P(n) \}$ is equal to $\mathbb{N}$, we follow the template:

1. (Base step) $P(1)$ is true;
2. (Inductive step) If for some $n$, $P(n)$ is true then $P(n + 1)$ is also true.

**PMI** guarantees that $S = \mathbb{N}$. 
Sequences

**Definition**
A sequence is a function $f$ whose domain is $\mathbb{N}$.

It can be represented as

$$\{f(1), f(2), f(3), \ldots\}$$

or

$$\{f(0), f(1), f(2), f(3), \ldots\}$$

or

$$\{f(n), \ldots, \ n \geq n_0\}$$

We will first examine sequences of real numbers, $f : \mathbb{N} \rightarrow \mathbb{R}$. 
Sequences with values in a ring

Let \( R \) be a ring and \( \mathcal{R} \) the set [actually a ring] of all sequences \( f : \mathbb{N} \rightarrow R \). The operations are:

\[
(a_1, a_2, a_3, \ldots) + (b_1, b_2, b_3, \ldots) = (a_1 + b_1, a_2 + b_2, a_3 + b_3, \ldots)
\]

\[
(a_1, a_2, a_3, \ldots) \times (b_1, b_2, b_3, \ldots) = (a_1 \cdot b_1, a_2 \cdot b_2, a_3 \cdot b_3, \ldots)
\]

This ring, sometimes denoted by \( R^\mathbb{N} \), is a direct product of copies of \( R \).

Note that we have also the operation

\[
 r(a_1, a_2, a_3, \ldots) = (ra_1, ra_2, ra_3, \ldots)
\]
Rings of Polynomials

Let us endow the set of sequences above with a different multiplication. For convenience we label the sequence as:

\[(a_0, a_1, a_2, a_3, \ldots), \quad a_i \in \mathbb{R}\]

\[(a_0, a_1, a_2, a_3, \ldots) \times (b_0, b_1, b_2, b_3, \ldots) = (c_0, c_1, c_2, c_3, \ldots)\]

\[
\begin{align*}
c_0 &= a_0b_0 \\
c_1 &= a_0b_1 + a_1b_0 \\
&\vdots \\
c_n &= \sum_{i+j=n} a_ib_j = a_0b_n + \cdots + a_nb_0
\end{align*}
\]
Special Sequences

\[ I = (1, 0, 0, 0, \ldots) \]
\[ x = (0, 1, 0, 0, \ldots) \]

\[ x = (0, 1, 0, 0, \ldots) \]
\[ x^2 = (0, 0, 1, 0, \ldots) \]
\[ x^3 = (0, 0, 0, 1, \ldots) \]

And most importantly

\[ (r_0, r_1, r_2, r_3, \ldots) = r_0 I + r_1 x + r_2 x^2 + r_3 x^3 + \ldots \]
Polynomials

Proposition

With the composition above:

1. The set of all sequences with values in \( \mathbb{R} \) is a ring, denoted \( \mathbb{R}[[x]] \).

2. The subset of all sequences \( \mathbf{f} \) such that \( \mathbf{f}(n) = 0 \) for all \( n \gg 0 \) is also a ring, called the ring of polynomials of \( \mathbb{R} \), and is denoted by \( \mathbb{R}[x] \).

As abelian groups:

1. \( \mathbb{R}[[x]] \cong \mathbb{R}^\mathbb{N} \)

2. \( \mathbb{R}[x] \cong \mathbb{R}^{\oplus \mathbb{N}} \)
Rings of Polynomials

Rings of polynomials in \( n \) indeterminates, \( n > 1 \), can be built on a similar construction: Let \( R \) be a ring

- Set \( \mathbb{N} = \{0, 1, 2, \ldots\} \) and \( \mathbb{M} = \mathbb{N}^n \) be the set \( \alpha = (\alpha_1, \ldots, \alpha_n) \). We refer to \( \deg \alpha = \alpha_1 + \cdots + \alpha_n \) as the total degree of \( \alpha \) (referred to as a multi-index).

- Let \( \mathcal{P}(n) \) the set of functions \( f: \mathbb{M} \to R \)

- Addition in \( \mathcal{P}(n) \) is defined by \( (f + g)(\alpha) = f(\alpha) + g(\alpha) \)
Multiplication in $\mathcal{P}(n)$ is defined by the convolution rule:
Note that for each $\gamma \in \mathbf{M}$ there are only finitely many pairs $(\alpha, \beta)$ such that
$$\gamma = \alpha + \beta$$

Define multiplication by
$$ (f \cdot g)(\gamma) = \sum_{\alpha + \beta = \gamma} f(\alpha) \cdot g(\beta) $$

**Proposition**

$\mathcal{P}(n)$ is a ring with these operations.
The elements of $\mathcal{P}(n)$ are called polynomials in $n$ indeterminates.

For a given multi-index $\alpha = (\alpha_1, \ldots, \alpha_n)$, the function $f$ such that $f(\alpha) = 1$ and $f(\beta) = 0$ for $\beta \neq \alpha$, is written

$$f = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$$

or simply $x^\alpha$. These functions are called monomials.

Every $f$ can be written as a finite sum

$$f = \sum_{\alpha} c_{\alpha} x^\alpha,$$

where $c_{\alpha}$ is a constant function.

Typically $f$ is a sum of several terms. It is called a binomial, trinomial etc if .... If $f$ has few terms it is called a fewnomial...
The ring $\mathcal{P}(2)$ is noteworthy.

- The set of functions $f : M \to R$ such that $f(m) = 0$ for almost all $m \in M$ that we used to get $\mathcal{P}(2)$ can be realized another way.

- Let $F : \mathbb{N} \to R[x]$ which is zero for almost all $r \in \mathbb{N}$. For each $r \in \mathbb{N}$, $F(r) \in R[x]$ means that $F(r) : \mathbb{N} \to R$ which is zero for almost all $s \in \mathbb{N}$, that is

$$F(r)(s) = 0$$

for almost all $(r, s) \in \mathbb{N}^2$. These are the functions used to define $\mathcal{P}(2)$.

- This shows that $\mathcal{P}(2) = R[x, y]$. More precisely, we must still verify that the two products coincide—which is easy.
Definition

A homomorphism \( \varphi : R \rightarrow R' \) from one ring to another is a map which is compatible with the laws of composition and which carries 1 to 1, that is, a map such that

\[
\varphi(a + b) = \varphi(a) + \varphi(b), \quad \varphi(ab) = \varphi(a)\varphi(b), \quad \varphi(1_R) = 1_{R'},
\]

for all \( a, b \in R \). An isomorphism of rings is bijective homomorphism. If there is an isomorphism \( R \rightarrow R' \), the two rings are said to be isomorphic.

Example

Let \( R = \mathbb{C} \). complex conjugation, \( a + bi \rightarrow a - bi \) is an isomorphism of \( \mathbb{C} \).
Matrix Rings

Let $R = M_n(\mathbb{R})$ be the ring of $n \times n$ real matrices, and let $A$ be an invertible matrix. Define

$$\varphi : R \to R, \quad \varphi(X) = AXA^{-1}$$

$$\varphi(I) = AIA^{-1} = I$$

$$\varphi(X + Y) = A(X + Y)A^{-1} = AXA^{-1} + AYA^{-1} = \varphi(X) + \varphi(Y)$$

$$\varphi(XY) = A(XY)A^{-1} = AXA^{-1}AYA^{-1} = \varphi(X)\varphi(Y)$$

Thus conjugation by $A$ is an isomorphism of $R$. 
The Substitution Principle

Proposition

Let \( \varphi : R \rightarrow R' \) be a ring homomorphism.

(a) Given an element \( \alpha \in R' \), there is a unique homomorphism \( \Phi : R[x] \rightarrow R' \) which agrees with the map \( \varphi \) on constant polynomials and which sends \( x \mapsto \alpha \).

(b) More generally, given elements \( \alpha_1, \ldots, \alpha_n \in R' \), there is a unique homomorphism \( \Phi : R[x_1, \ldots, x_n] \rightarrow R' \) from the polynomial ring in \( n \) variables to \( R' \), which agrees with \( \varphi \) on constant polynomials and which sends \( x_\nu \mapsto \alpha_\nu \), for \( \nu = 1, \ldots, n \).
Proof. If $\Phi$ exists,

$$\Phi(a_n x^n + \cdots + a_0) = \Phi(a_n)\Phi(x^n) + \cdots + \Phi(a_0) = \varphi(a_n)\alpha^n + \cdots + \varphi(a_0)$$

Thus $\Phi$ is uniquely defined by $\varphi$ and $\Phi(x) = \alpha$.

To prove the existence, we define $\Phi$ by the formula above, and check that

$$\Phi(f(x)+g(x)) = \Phi(f(x))+\Phi(g(x)), \quad \Phi(f(x)g(x)) = \Phi(f(x))\Phi(g(x))$$

Having done this so many times in Calculus, we believe.
Corollary

Let \( x = (x_1, \ldots, x_m) \) and \( y = (y_1, \ldots, y_n) \) denote sets of variables. There is a unique isomorphism \( R[x, y] \rightarrow R[x][y] \) which is the identity on \( R \) and which sends the variables to themselves.
Proposition

Let $\mathcal{R}$ denote the ring of continuous real-valued functions on $\mathbb{R}^n$. The map $\varphi : \mathbb{R}[x_1, \ldots, x_n] \to \mathcal{R}$ sending a polynomial to its associated polynomial function is an injective homomorphism.
Proposition

There is exactly one homomorphism

$$
\varphi : \mathbb{Z} \rightarrow R
$$

from the ring of integers to an arbitrary ring R. It is the map defined by

$$
\varphi(n) = 1_R + \cdots + 1_R \text{ (}n\text{ times)} \text{ if } n > 0, \text{ and } \\
\varphi(-n) = -\varphi(n).
$$
The property of the kernel of a ring homomorphism – that it is closed under multiplication by arbitrary elements of the ring – is abstracted in the concept of an ideal.

**Definition**

An ideal $I$ of a ring $R$ is a subset of $R$ with these properties:

- (i) $I$ is a subgroup of $R^+$;
- (ii) If $a \in I$ and $r \in R$, then $ra \in I$.

**Example**

Let $R$ be a commutative ring and $x \in R$. The set of multiples of $x$, $Rx = \{ra; r \in R\}$, is an ideal. It is called a principal, or one-generated ideal.
Example

If $R$ is a ring and $S = \{a_1, \ldots, a_n\}$ is a set of elements of $R$, the set of all combinations

$$r_1a_1 + \cdots + r_na_n, \quad r_i \in R$$

is an ideal. It is called the ideal generated, or spanned, by $S$.

If $R$ is not commutative, there are other notions of ideals:

- $I$ is a **left ideal** if $I$ is a subgroup of $R^+$, and for every $a \in I$, $r \in R$, $ra \in I$.
- $I$ is a **right ideal** if $I$ is a subgroup of $R^+$, and for every $a \in I$, $r \in R$, $ar \in I$.
- $I$ is a **two-sided ideal** if $I$ is a subgroup of $R^+$, and for every $a \in I$, $r, s \in R$, $ras \in I$. 
Ideals of Fields

Proposition

(a) Let $F$ be a field. The only ideals of $F$ are the zero ideal and the unit ideal.

(b) Conversely, if a ring $R$ has exactly two ideals, then $R$ is a field.

Proof.

(a) Let $I$ be a nonzero ideal. If $0 \neq a \in I$, since $F$ is a field, $a^{-1} \in F \implies 1 = a^{-1}a \in I$. Thus $I = R$.

(b) If $0 \neq a$, $Ra$ is a nonzero ideal, so $Ra = R$, which means there $r \in R$ such that $ra = 1$.
Corollary

Let $F$ be a field and let $R'$ be a nonzero ring. Every homomorphism $\varphi : F \to R'$ is injective.

Proof.

Let $I$ be $\ker \varphi$. Since $\varphi(1_F) = 1_R$, $\varphi$ is not the null mapping, and thus its kernel $\neq F$. But the only other ideal of $F$ is $(0)$. □
The ideals of $\mathbb{Z}$

**Proposition**

Every ideal in the ring $\mathbb{Z}$ of integers is a principal ideal.

**Proof.**

Every ideal $I$ of $\mathbb{Z}$ is a subgroup of $\mathbb{Z}^+$. But we have already seen that the subgroups of $\mathbb{Z}$ are cyclic, that is $I = \mathbb{Z}a$, for some integer $a$. Note $\mathbb{Z}a$ is also closed multiplication by elements of $\mathbb{Z}$. 

Long Division Algorithm

Proposition

Let $R$ be a ring and let $f, g$ be polynomials in $R[x]$. Assume that the leading coefficient of $f$ is a unit in $R$. (This is true, for instance, if $f$ is a monic polynomial.) Then there are polynomials $q, r \in R[x]$ such that

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

and such that the degree of the remainder $r$ is less than the degree of $f$ or else $r = 0$.

Proof. We may assume that $\deg g(x) \geq \deg f(x)$, as otherwise there is nothing to prove. We are going to induction on $\deg g(x)$ assuming that the assertion is true for polynomials of lesser degree.
\[ g(x) = b_m x^m + \text{lower degree} \]
\[ f(x) = a_n x^n + \text{lower degree} \]

By assumption \( u = a_n \) is invertible. Note that

\[
h(x) = g(x) - b_m u^{-1} x^{m-n} f(x)
\]

satisfies \( \deg h(x) < \deg g(x) \).
By induction we have

\[ h(x) = f(x)q'(x) + r(x), \quad \deg r(x) < \deg f(x) \]

and therefore

\[ g(x) = f(x)(q'(x) + b_m u^{-1} x^{m-n}) + r(x), \quad \deg r(x) < \deg f(x) \]

**Corollary**

Let \( g(x) \) be a monic polynomial in \( R[x] \), and let \( \alpha \) be an element of \( R \) such that \( g(\alpha) = 0 \). Then \( x - \alpha \) divides \( g \) in \( R[x] \).
Proposition

Let $F$ be a field. Every ideal in the ring $F[x]$ of polynomials in a single variable $x$ is a principal ideal.

**Proof.** Let $I$ be an ideal of $F[x]$. If $I = (0)$ there is nothing to prove.

If $I \neq (0)$, let $f(x)$ be a nonzero polynomial of least degree. We claim that every element $g(x)$ of $I$ is a multiple of $f(x)$. If $g(x) = 0$, there is nothing to do, so assume $g(x) \neq 0$. Since the leading coefficient of $f(x)$ is invertible, by the Long Division Algorithm there are polynomials $q(x)$ and $r(x)$ such that

$$g(x) = f(x)q(x) + r(x), \quad \deg r(x) < \deg f(x)$$

But $r(x) = g(x) - f(x)q(x)$ is an element of $I$, so must be 0 by the choice of $f(x)$. 
Corollary

Let $F$ be a field, and let $f$ and $g$ be polynomials which are not both zero. There is a unique monic polynomial $d(x)$ called the greatest common divisor of $f$ and $g$, with the following properties:

1. $d$ generates the ideal $(f, g)$ of $F[x]$ generated by the two polynomials $f, g$.
2. $d$ divides $f$ and $g$.
3. If $h$ is any divisor of $f$ and $g$, then $h$ divides $d$.
4. There are polynomials $p, q \in F[x]$ such that $d = pf + qg$.

Recall: The ideal $(f, g)$ is made up of all combinations

$$a(x)f(x) + b(x)g(x)$$
Radical of an Ideal

**Definition**

Let $I$ be an ideal of the commutative ring $R$. The *radical* of $I$ is the set

$$\sqrt{I} = \{ x \in R : x^n \in I \text{ some } n = n(x) \}.$$ 

**Proposition**

$\sqrt{I}$ is an ideal.

**Proof.**

If $a, b \in \sqrt{I}$, $a^m \in I$, $b^n \in I$, then

$$(a + b)^{m+n-1} = \sum_{i+j=m+n-1} \binom{m+n-1}{i} a^i b^j \in I,$$

since $i \geq m$ or $j \geq n$. 

**Principal Ideal Ring**

**Definition**

A ring \( R \) is a principal ideal ring if every ideal \( I \) is generated by one element, \( I = \{ ra : r \in R \} \).

- \( \mathbb{Z} \) and \( F[x] \) where \( F \) is a field are principal ideal rings.
- \( R = F[x, y] \) is not: The ideal \( I \) generated by \( x, y \) cannot be generated by 1 element.
Idempotents

Let $\mathbb{R} = \mathbb{Z}_6$ and consider the element $z = 3$. Note $z^2 = 9 = 3 = z$. These elements are called:

**Definition**
The element $e \in \mathbb{R}$ is called **idempotent** if $e^2 = e$.

**Definition**
$\mathbb{R}$ is a **Boolean** ring if $z^2 = z$ for all $z \in \mathbb{R}$.

**Proposition**

*If $\mathbb{R}$ is a Boolean ring, then*

1. $2z = 0$ for $z \in \mathbb{R}$;
2. If $a, b \in \mathbb{R}$, then $a, b$ are multiples of $a + b - ab$.

**Class proof**
Example: Boolean ring

For a non-empty set $X$ let $R$ the set of all functions $f : X \rightarrow \mathbb{Z}_2$.

- $(f + g)(s) = f(s) + g(s)$, and
- $(f \cdot g)(s) = f(s) \cdot g(s)$, define a ring structure on $R$.
- $f^2(s) = f(s) \cdot f(s) = f(s)$, so $R$ is Boolean.
Outline

1. Rings
2. Integers and Polynomials
3. Homomorphisms
4. Quotient rings and relations in a ring
5. Integral Domains and Rings of Fractions
6. Homework #10
7. Maximal Ideals
8. Noetherian Rings
9. Algebraic Geometry
10. Diagonalization
11. Diagonalization and Minimal Polynomials
12. Homework #11
Quotient rings

The most effective method to build new rings is the following:

Let $I$ be a two-sided proper ideal of the $R$ and denote by $\overline{R} = R/I$ the corresponding cosets $\{a + I : a \in R\}$. It defines on $\overline{R}$ an abelian group structure called the **quotient ring** $R/I$:

$$(a + I) + (b + I) = (a + b) + I$$
We claim that this operation and

$$(a + I) \times (b + I) = ab + I$$

defines a ring structure. Let us verify that if $a' + I = a + I$ and $b + I = b' + I$, then $ab + I = a'b' + I$: Since $a' = a + r$, $b' = b + s$, with $r, s \in I$

$$a'b' = (a + r)(b + s) = ab + (rb + sa + rs)$$

and thus $a'b'$ and $ab$ live in the same coset.

The axioms of associativity and distributivity are easily verified.

This is a source to many new rings
Example

Let $R = \mathbb{Z}$ and $I = \mathbb{Z}n$. Then $R/I$ is the ring of integers modulo $n$. 
Examples: Quotient rings

\((2) \subset \mathbb{Z} \Rightarrow \mathbb{Z}_2 = \mathbb{Z}/(2)\)

\((x^2 + x + 1) \subset \mathbb{Z}_2[x] \Rightarrow \mathbb{Z}_2[x]/(x^2 + x + 1) = \mathbb{F}_4\)

\((x^2 + 1) \subset \mathbb{R}[x] \Rightarrow \mathbb{C} = \mathbb{R}[x]/(x^2 + 1)\)

\((1 + 3i) \subset \mathbb{Z}[i] \Rightarrow \mathbb{Z}_{10} = R = \mathbb{Z}[i]/(1 + 3i)\)

Will check out some of these soon.
Theorem

Let $I$ be an ideal of a ring $R$.

(a) There is a unique ring structure on the set of cosets $\overline{R} = R/I$ such that the canonical map $\pi : R \to \overline{R}$ sending $a \mapsto \overline{a} = a + I$ is a homomorphism.

(b) The kernel of $\pi$ is $I$. 

Mapping property of quotient rings

**Proposition**

Let $f : R \rightarrow R'$ be a ring homomorphism with kernel $I$ and let $J$ be an ideal which is contained in $I$. Denote the residue ring $R/J$ by $\overline{R}$.

(a) There is a unique homomorphism $\overline{f} : \overline{R} \rightarrow R'$ such that $\overline{f}\pi = f$:

(b) *(First Isomorphism Theorem)* If $J = I$, then $\overline{f}$ maps $\overline{R}$ isomorphically to the image of $f$. 
Correspondence Theorem

Proposition

Let $\overline{R} = R/J$, and let $\pi$ denote the canonical map $R \to \overline{R}$.

(a) There is a bijective correspondence between the set of ideals of $R$ which contain $J$ and the set of all ideals of $\overline{R}$, given by

$$I \mapsto \pi(I), \quad \text{and} \quad \pi^{-1}(I) \mapsto \overline{I}.$$  

(b) If $I \subset R$ corresponds to $\overline{I} \subset \overline{R}$, then $R/I$ and $\overline{R}/\overline{I}$ are isomorphic rings.
\[ \mathbb{Z}[i]/(1 + 3i) \cong \mathbb{Z}/(10) \]

**Proposition**

The ring \( \mathbb{Z}[i]/(1 + 3i) \) is isomorphic to the ring \( \mathbb{Z}/10\mathbb{Z} \) of integers modulo 10.

**Proof.** Consider the homomorphism

\[ \varphi : \mathbb{Z} \to \mathbb{Z}[i] \to R = \mathbb{Z}[i]/(1 + 3i) \]

induced by the embedding of \( \mathbb{Z} \) in \( \mathbb{Z}[i] \). We claim that \( \varphi \) is a surjection of kernel 10\( \mathbb{Z} \):

\[
1 + 3i \equiv 0 \Rightarrow i(1 + 3i) \equiv 0 \Rightarrow i - 3 \equiv 0 \Rightarrow i \equiv 3
\]

\[ a + bi \equiv a + 3b \Rightarrow \varphi \text{ is surjection} \]

For \( n \) in kernel of \( \varphi \),

\[
n = z(1 + 3i) = (a + bi)(1 + 31)
\]

\[
= (a - 3b) + (3a + b)i \quad \Rightarrow \quad b = -3a \quad \Rightarrow \quad n = 10a
\]
The Circle Ring

**Proposition**

\[ \mathbb{R}[x, y]/(x^2 + y^2 - 1) \cong \mathbb{R}[\cos t, \sin t]. \]

The ring \( R = \mathbb{R}[x, y]/(x^2 + y^2 - 1) \): known as the **circle ring**

- Consider the natural homomorphism
  
  \[ f : \mathbb{R}[x, y] \rightarrow \mathbb{R}[\cos t, \sin t], \quad f(x) = \cos t, \ f(y) = \sin t \]
  
  \( \mathbb{R}[\cos t, \sin t] \) is the ring of trigonometric polynomials.

- \( f(x^2 + y^2 - 1) = 0 \) so there is an induced surjection
  
  \[ \varphi : \mathbb{R}[x, y]/(x^2 + y^2 - 1) \rightarrow \mathbb{R}[\cos t, \sin t] \]

- \( \varphi \) is an isomorphism because: (i) \( \mathbb{R}[\cos t, \sin t] \) is an infinite dimensional \( \mathbb{R} \)-vector space (why?); for any ideal \( L \) larger than \( (x^2 + y^2 - 1) \), \( \mathbb{R}[x, y]/L \) is a finite dimensional \( \mathbb{R} \)-vector space (why?).
Proposition

The ring $\mathbb{R}[x, y]/(xy)$ is isomorphic to the subring of the product ring $\mathbb{R}[x] \times \mathbb{R}[y]$ consisting of the pairs $(p(x), q(y))$ such that $p(0) = q(0)$.

Proof. Let us sketch the proof, leaving the details to reader:

$$\mathbb{R}[x, y]/(xy) \cong \{(p(x), q(y)) : p(0) = q(0)\}$$

Consider the homomorphism

$$\varphi : \mathbb{R}[x, y]/(xy) \to \mathbb{R}[x, y]/(y) \times \mathbb{R}[x, y]/(x)$$

$$\varphi(a + (xy)) = (a + (y), a + (x))$$

Check that $\varphi$ is one-one and determine its image.
Outline

1. Rings
2. Integers and Polynomials
3. Homomorphisms
4. Quotient rings and relations in a ring
5. Integral Domains and Rings of Fractions
6. Homework #10
7. Maximal Ideals
8. Noetherian Rings
9. Algebraic Geometry
10. Diagonalization
11. Diagonalization and Minimal Polynomials
12. Homework #11
**Definition**

An **integral domain** $R$ is a nonzero ring having no zero divisors. That is, if $ab = 0$, then $a = 0$ or $b = 0$.

**Example**

Any subring $R$ of a field $F$ is an integral domain.
Properties

Proposition

1. If $R$ is an integral domain then the polynomial ring $R[x]$ is also an integral domain.

2. An integral domain with finitely many elements is a field.

Proof. Class proof.
Embedding

**Theorem**

Let $\mathbf{R}$ be an integral domain. There exists an embedding of $\mathbf{R}$ into a field, meaning an injective homomorphism $\varphi : \mathbf{R} \to \mathbf{F}$, where $\mathbf{F}$ is a field.

**Proof.** We are going to build fractions with the elements of $\mathbf{R}$.

- Let $S$ be the set of all ordered pairs $(a, b), \ a, b \in \mathbf{R}, \ b \neq 0$. Define the following relation on $S$:

  $$(a, b) \sim (c, d) \iff ad = bc$$

- **Claim:** $\sim$ is an equivalence relation.
  - reflexive: $(a, b) \sim (a, b)$ clear
  - symmetric: $(a, b) \sim (c, d) \iff (c, d) \sim (a, b)$
  - transitive: $(a, b) \sim (c, d) \sim (e, f) \Rightarrow$

    $$ad = bc, cf = de \Rightarrow adf = bcfbcf = bde \Rightarrow af = be$$
Field of fractions

Let \( F \) be the set of equivalence classes. We denote the equivalence of \((a, b)\) by \( a/b \).

- We define a field structure on \( F \) by the rules:

\[
(a/b)(c/d) = ac/bd, \quad a/b + c/d = \frac{ad + bc}{cd}
\]

- It must be verified that these definitions do not depend on the representative taken, for instance, if \( a/b = a'/b' \), then \((a/b)(c/d) = (a/b')(c/d)\). We believe!

- With these rules, \( F \) is a field. For instance, if \( a/b \) is such that \( a \neq 0 \), then \((a/b)^{-1} = (b/a)\).

- Finally, define \( \varphi : \mathbb{R} \rightarrow F \) by the rule \( \varphi(a) = a/1 \). It is easy to verify that \( \varphi \) is an injective homomorphism.
Examples

- What are fractions in $\mathbb{Q}$?
- $\mathbb{Z} \rightarrow \mathbb{Q}$
- $\mathbb{R}[x] \rightarrow \mathbb{R}(x) : \frac{p(x)}{q(x)}$
Class Exercise

Proposition

Let $\mathbf{R}$ be an integral domain, with field of fractions $\mathbf{F}$, and let $\varphi : \mathbf{R} \to \mathbf{K}$ be an injective homomorphism of $\mathbf{R}$ to the field $\mathbf{K}$. Then the rule

$$\Phi(a/b) = \varphi(a)\varphi(b)^{-1}$$

defines the unique extension of $\varphi$ to a homomorphism $\Phi : \mathbf{F} \to \mathbf{K}$. 
Outline

1. Rings
2. Integers and Polynomials
3. Homomorphisms
4. Quotient rings and relations in a ring
5. Integral Domains and Rings of Fractions
6. Homework #10
7. Maximal Ideals
8. Noetherian Rings
9. Algebraic Geometry
10. Diagonalization
11. Diagonalization and Minimal Polynomials
12. Homework #11
1. If $R$ is a Boolean ring, prove that every finitely generated ideal $I$ is generated by one element.

2. If $R$ is a finite Boolean ring, $|R| = 2^n$, for some integer $n$. 
   *Hint:* For each $e \in R$, show that $R = Re \times R(1 - e)$. Note that $Re$ is a Boolean ring with identity $e$.

3. Prove that if $R$ is a finite integral domain then:
   - $R$ is a field;
   - $R$ contains a subfield $\mathbb{Z}_p$, for some prime $p$;
   - $|R| = p^n$

4. Let $R_1, R_2$ be two rings. Describe the ideals of $R_1 \times R_2$ in terms of the ideals of $R_1$ and $R_2$. 

---

Homework #10

---

Rings  Integers and Polynomials  Homomorphisms  Quotient rings and relations in a ring  Integral Domains and Rings of...
Outline

1. Rings
2. Integers and Polynomials
3. Homomorphisms
4. Quotient rings and relations in a ring
5. Integral Domains and Rings of Fractions
6. Homework #10
7. **Maximal Ideals**
8. Noetherian Rings
9. Algebraic Geometry
10. Diagonalization
11. Diagonalization and Minimal Polynomials
12. Homework #11
Maximal Ideals

Definition
An ideal $M$ is maximal if $M \neq \mathbb{R}$ but $M$ is not contained in any ideals other than $M$ or $\mathbb{R}$.

Proposition
1. An ideal $M$ of a ring $\mathbb{R}$ is maximal iff $\overline{\mathbb{R}} = \mathbb{R}/M$ is a field.
2. The zero ideal of $\mathbb{R}$ is maximal iff $\mathbb{R}$ is a field.
Examples

Proposition

The maximal ideals of \( \mathbb{Z} \) are the ideals \((p)\), where \( p \) is a nonzero prime number.

Proposition

The maximal ideals of the ring \( \mathbb{C}[x] \) of complex polynomials are the ideals \((f(x))\) where \( f(x) = x - c \), were \( c \in \mathbb{C} \).

Proof.

Let \( M \) be a maximal ideal; clearly \( M \neq (0) \). We know that \( \mathbb{C}[x] \) is a principal ideal ring that every ideal is generated by a single polynomial, \( M = (f(x)) \). If \( \deg(f(x)) > 1 \), and \( c \) is a root, \( f(x) = (x - c)g(x) \).

It follows that \( M \subset (x - c) \). Since \( M \) is maximal, \( M = (x - c) \).
Example

Let $\mathbb{R} = \mathbb{R}[x, y]$, the ring of polynomials in two indeterminates over $\mathbb{R}$. Define a homomorphism

$$\varphi : \mathbb{R} \to \mathbb{C}, \quad x \to i, \ y \to i$$

Let $M$ be the kernel. Note that $x - y \to 0$ and $x^2 + 1 \to 0$, and $r \to r$ if $r \in \mathbb{R}$

Note that $\varphi$ is surjective, so $\mathbb{R}/M \cong \mathbb{C}$. Therefore $M$ is maximal. **Claim:** $M = (x - y, x^2 + 1)$. 
Example from Analysis

Let $\mathbf{R}$ be the ring of real continuous functions on the interval $I = [0, 1]$. For each $a \in I$, the evaluation $f(x) \mapsto f(a)$ defines a surjective homomorphism

$$\varphi : \mathbf{R} \to \mathbf{R}$$

The kernel is $M = \{f(x) : f(a) = 0\}$. Since $\mathbf{R}/M \simeq \mathbf{R}$, $M$ is a maximal ideal.

Now we are going to use hard analysis to prove the converse. We are going to use the fact that the interval $I$ is compact: any covering

$$I \subset \bigcup (a_i, b_i)$$

has a finite subcover.
For maximal ideal $M$ of the ring $\mathbb{R}$ of continuous functions on $I = [0, 1]$ there is $a \in I$ such that $M = \{f(x) : f(a) = 0\}$.

**Proof.** Deny it. This means that for each $a \in I$ there is $f(x) \in M$ such that $f(a) \neq 0$. Since $f(x)$ is continuous with $f(a) \neq 0$, in a small interval $(c, d)$ about $a$, $f(x) \neq 0$ for $x \in (c, d)$.

This gives rise to a covering

$$I \subset \bigcup_{i=1}^{n} (c_i, d_i)$$

by such intervals (actually a finite collection) and functions $f_i(x) \in M$ nonvanishing on $(c_i, d_i)$.
Consider the function

\[ f(x) = \sum_{i=1}^{n} f_i(x)^2 \]

\( f \in M \) and does not vanish anywhere in \( I \). This implies that \( 1/f(x) \in R \), and therefore \( 1 = (1/f(x))f(x) \in M \), a contradiction.
Prime Ideals

Definition
Let $R$ be a commutative ring. An ideal $P$ of $R$ is prime if $P \neq R$ and whenever $a \cdot b \in P$ then $a \in P$ or $b \in P$.

Equivalently:

- $R/P$ is an integral domain
- If $I$ and $J$ are ideals and $I \cdot J \subseteq P$ then $I \subseteq P$ or $J \subseteq P$
Prime ideals and homomorphisms

prime ideals of $R$  morphisms $\varphi : R \rightarrow S$
Prime ideals arise in issues of factorization and very importantly:

**Proposition**

Let $\phi : R \rightarrow S$ be a homomorphism of commutative ring. If $S$ is an integral domain, then $P = \ker(\phi)$ is a prime ideal. More generally, if $S$ is an arbitrary commutative ring and $Q$ is a prime ideal, then $P = \phi^{-1}(Q)$ is a prime ideal of $R$.

**Proof.** Inspect the diagram
Exercise

Consider the homomorphism of rings

\[ \varphi : k[x, y, z] \rightarrow k[t] \]
\[ x \rightarrow t^3 \]
\[ y \rightarrow t^4 \]
\[ z \rightarrow t^5 \]

Let \( P \) be the kernel of this morphism. Note that \( x^3 - yz, y^2 - xz \) and \( z^2 - x^2y \) lie in \( P \).

**Task:** Prove that \( P \) is generated by these 3 polynomials.

**Task:** Describe the prime ideals of the ring

\[ R = \mathbb{C}[x, y]/(y^2 - x(x - 1)(x - 2)). \]
Significance: Prime and Maximal Ideals

These ideals give rise to new interesting rings:

- Prime ideals are significant because: $R/P$ is a domain
- Maximal ideals are significant because: $R/P$ is a field
- In particular maximal ideals are prime
Let $\mathbb{R}$ be a ring. Given a proper ideal $I$, how to add something to it an still get a proper ideal?

- If $a \notin I$, add $a$ to $I$, which means form all $ra + s$, $r \in \mathbb{R}$, $s \in I$.

- This ideal, $(a, I)$, may be improper, $(a, I) = \mathbb{R}$, that is we have a term $ra + s = 1$. Hard to predict.
A theorem for believers

**Theorem**

Let $\mathbf{R}$ be a ring. Every ideal $I$ of $\mathbf{R}$ which is not the unit ideal is contained in a maximal ideal.

How we are going to do this?

**Proof.** [?]  

- Let $I$ be an ideal. If $I$ is maximal, we are done.
- If not, there is a larger proper ideal $I \subset I_1$. If $I_1$ is maximal,...
- In this manner we get a chain of proper ideals $I \subset I_1 \subset \cdots \subset I_n \subset$  
- Observation: $\bigcup_n I_n$ is a proper ideal—obviously closed under addition, multiplication and 1 is not in the union.  
What else can we do?
Zorn Lemma

This is an extra axiom which when added to the more common axioms of mathematics asserts:

Any subset \( Y \) of a partially ordered set \( X \) such the chains of elements of \( Y \) have a supremum has maximal elements
Outline

1. Rings
2. Integers and Polynomials
3. Homomorphisms
4. Quotient rings and relations in a ring
5. Integral Domains and Rings of Fractions
6. Homework #10
7. Maximal Ideals
8. Noetherian Rings
9. Algebraic Geometry
10. Diagonalization
11. Diagonalization and Minimal Polynomials
12. Homework #11
Emmy Noether (1882-1935)

http://upload.wikimedia.org/wikipedia/commons/e/e5/Noether.jpg
Noetherian Rings

**Definition**

\( R \) is a **Noetherian** if every ascending chain of ideals is stationary, that is \( A_n = A_{n+1} = \ldots \) from a certain point on.

**Definition**

The ring \( R \) has the **Maximal Condition** if every subset \( S \) of the \( X \) (set of ideals ordered by inclusion) contains a **maximum submodule**
Example

Let $R = \mathbb{Z}$: a chain of ideals

$$(a_1) \subset (a_2) \subset \cdots \subset (a_n)$$

means a sequence of integers $a_2 | a_1$, $a_3 | a_2$, $\ldots$, each dividing the preceding, in a process that must stop. The same argument applies of the ring $R = F[x]$, where $F$ is a field.
Proposition

\textbf{R} is a Noetherian ring iff \textbf{R} has the Maximal Condition.

\textbf{Proof.} Let \( S \) be a set of ideals of \( \textbf{R} \). If \( S \) contains no maximal element, we can build an ascending chain

\[
A_1 \subset A_2 \subset \cdots \subset A_n \subset \cdots
\]

contradicting the assumption that \( \textbf{R} \) is Noetherian. The converse has a similar proof.
Proposition

\textbf{R} is Noetherian iff every ideal is finitely generated.

\textbf{Proof.} Suppose \textbf{R} is Noetherian. Let us deny. Let \( A \) be an ideal of \textbf{R} and assume it is not finitely generated. It would permit the construction of an increasing sequence of submodules of \( A \),

\[(a_1) \subset (a_1, a_2) \subset \cdots \subset (a_1, a_2, \ldots, a_n) \subset \cdots ,\]

\(a_{n+1} \in A \setminus (a_1, \ldots, a_n)\).

Conversely if \( A_1 \subseteq A_2 \subseteq \cdots \) is an increasing sequence of ideals, let \( B = \bigcup_{i \geq 1} A_i \) is an ideal and therefore \( B = (b_1, \ldots, b_m) \).

Each \( b_i \in A_{n_i} \) for some \( n_i \). If \( n = \max\{n_i\}, A_n = A_{n+1} = \cdots \).
Hilbert Basis Theorem

Theorem (HBT)

If $R$ is Noetherian then $R[x]$ is Noetherian.

1. If $R$ is Noetherian and $x_1, \ldots, x_n$ is a set of independent indeterminates, then $R[x_1, \ldots, x_n]$ is Noetherian.

2. $\mathbb{Z}[x_1, \ldots, x_n]$ is Noetherian.

3. If $k$ is a field, then $k[x_1, \ldots, x_n]$ is Noetherian.
Proof of the HBT

Suppose the \( R[x] \)-ideal \( I \) is not finitely generated. Let \( 0 \neq f_1(x) \in I \) be a polynomial of smallest degree, \( f_1(x) = a_1x^{d_1} + \text{lower degree terms} \).

Since \( I \neq (f_1(x)) \), let \( f_2(x) \in I \setminus (f_1(x)) \) of least degree. In this manner we get a sequence of polynomials

\[
f_i(x) = a_ix^{d_i} + \text{lower degree terms},
\]

\[
f_i(x) \in I \setminus (f_1(x), \ldots, f_{i-1}(x)), \quad d_1 \leq d_2 \leq d_3 \leq \cdots
\]

Set \( J = (a_1, a_2, \ldots) = (a_1, a_2, \ldots, a_m) \subseteq R \).
Let \( f_{m+1}(x) = a_{m+1}x^{d_{m+1}} + \text{lower degree terms} \). Then

\[
a_{m+1} = \sum_{i=1}^{m} s_i a_i, \quad s_i \in R.
\]

Consider

\[
g(x) = f_{m+1} - \sum_{i=1}^{m} s_i x^{d_{m+1} - d_i} f_i(x).
\]

\( g(x) \in I \setminus \langle f_1(x), \ldots, f_m(x) \rangle \), but \( \deg g(x) < \deg f_{m+1}(x) \), which is a contradiction.
Examples

- \( \mathbb{Z} \) is Noetherian, so is \( R = \mathbb{Z}[x_1, \ldots, x_n] \)
- A field \( F \) is Noetherian, so is \( R = F[x_1, \ldots, x_n] \)
- \( A \) is Noetherian, so is \( R = A[x_1, \ldots, x_n]/I \)
Power Series Rings

Another construction over a ring $R$ is that of the power series ring $R[[x]]$:

$$f(x) = \sum_{n \geq 0} a_n x^n, \quad g(x) = \sum_{n \geq 0} b_n x^n$$

with addition component wise and multiplication the Cauchy operation

$$f(x)g(x) = h(x) = \sum_{n \geq 0} c_n x^n$$

$$c_n = \sum_{i+j=n} a_i b_{n-i}$$

**Theorem**

*If $R$ is Noetherian then $R[[x]]$ is Noetherian.*
Proposition

A commutative ring \( R \) is Noetherian iff every prime ideal is finitely generated.

Proof. If \( R \) is not Noetherian, there is an ideal \( I \) maximum with the property of not being finitely generated (Zorn’s Lemma). We assume \( I \) is not prime, that is there exist \( a, b \notin I \) such that \( ab \in I \).
The ideals \((I, a)\) and \((I : a)\) are both larger than \(I\) and therefore are finitely generated:

\[
(I : a) = (a_1, \ldots, a_n) \\
(I, a) = (b_1, \ldots, b_m, a), \quad b_i \in I
\]

**Claim:** \(I = (b_1, \ldots, b_m, a, a_1, \ldots, a_n)\)

If \(c \in I\),

\[
c = \sum_{i=1}^{m} c_i b_i + ra, \quad r \in I : a
\]
Proof. Let $P$ be a prime ideal of $R[[x]]$. Set $p = P \cap R$. $p$ is a prime ideal of $R$ and therefore it is finitely generated.

Denote by $p[[x]] = pR[[x]]$ the ideal of $R[[x]]$ generated by the elements of $p$. It consists of the power series with coefficients in $p$ and $R[[x]]/p[[x]]$ is the power series ring $R/p[[x]]$.

We have the embedding

$$P' = P/p[[x]] \hookrightarrow (R/p)[[x]]$$

$P'$ is a prime ideal of $R/p[[x]]$ and $P' \cap R/p = 0$. It will suffice to show that $P'$ is finitely generated.
We have reduced the proof to the case of a prime ideal \( P \subset R[[x]] \) and \( P \cap R = (0) \).

If \( x \in P \), \( P = (x) \) and we are done.
For \( f(x) = a_0 + a_1 x + \cdots \in P \), let \( J = (b_1, \ldots, b_m) \subset R \) be the ideal generated by all \( a_0 \),

\[ f_i = b_i + \text{higher terms} \in P. \]

**Claim:** \( P = (f_1, \ldots, f_m) \).

From \( a_0 = \sum_i s_i^{(0)} b_i \), we write

\[ f(x) - \sum_i s_i^{(0)} f_i = xh \quad \Rightarrow h \in P. \]
We repeat with $h$ and write

$$f(x) = \sum_i s_i^{(0)} f_i + x \sum_i s_i^{(1)} f_i + x^2 g, \quad g \in P.$$ 

Iterating we obtain

$$f(x) = \sum_i (s_i^{(0)} + s_i^{(1)} x + s_i^{(2)} x^2 + \cdots) f_i.$$
What is Algebraic Geometry?

Needs lots of space [it is, in fact, about Space] to describe all it is about.
David Hilbert (1862-1943)

Mathematician
Algebraist
Topologist
Geometrist
Number Theorist
Physicist
Analyst
Philosopher
Genius
And modest too...

"Physics is much too hard for physicists." - Hilbert, 1912
Do polynomials have roots?

Let $f(x) = f(x_1, \ldots, x_n)$ be a nonconstant polynomial of $R = \mathbb{C}[x] = \mathbb{C}[x_1, \ldots, x_n]$, $n > 1$.

**Fact:** There is $c \in \mathbb{C}^n$ such that $f(c) = 0$.

The answer is easy when

$$f(x_1, \ldots, x_n) = x_n^d + g(x_1, \ldots, x_n),$$

where $g(x)$ is a polynomial of degree $< d$ in the variable $x_n$.

For example: Discuss

$$x^6 + yx^5 + y^8 + 1$$
More generally, let $f_1(x), \ldots, f_m(x)$ be a set of elements of $R = \mathbb{C}[x]$.

**Question:** What are the obstructions to finding $c \in \mathbb{C}^n$ such that

$$f_1(c) = f_2(c) = \cdots = f_m(c) = 0 ?$$

Obviously one is: there exist $g_1(x), \ldots, g_m(x)$ such that

$$g_1(x)f_1(x) + \cdots + g_m(x)f_m(x) = 1$$

**What else?**
Volunteer!

- Sketch the graph of the equation

  \[ y^2 = x(x - 1)(x - 2) \]

- Can you see a group in the graph?
Let $k$ be a field and denote by $\overline{k}$ its algebraic closure. (What are these? Like $\mathbb{R}$ and $\mathbb{C}$) We stay with $\mathbb{C}$.

The Hilbert Nullstellensatz is about qualitative results on systems of polynomial equations.

Let $f_i(x_1, \ldots, x_n) \in R = k[x_1, \ldots, x_n], 1 \leq i \leq m$, be a set of polynomials.

**Definition**

The algebraic variety defined by the $f_i$ is the set of zeros

\[ V(f_1, \ldots, f_m) = \{ c = (c_1, \ldots, c_n) \in \mathbb{C}^n : f_i(c) = 0, \quad 1 \leq i \leq m \}. \]

A hypersurface is a variety defined by a single equation $V(f)$. If $I$ is the ideal generated by the $f_i$, then the variety defined by $I$ is $V(I) = V(f_1, \ldots, f_m)$. 
Notes about $\mathbb{C}$

- $\mathbb{C}$ is a two-dimensional vector space over $\mathbb{R}$

- If $\mathbb{C} \subset \mathbb{F}$ is a field that is of finite dimension over $\mathbb{C}$, obviously it is of (double) finite dimension over $\mathbb{R}$

- This means that if $u \in \mathbb{F}$, the vector subspace spanned by the powers of $u$, 
  
  \[ 1, u, u^2, \ldots, \]

  is finite dimensional over $\mathbb{R}$ and thus there must be a polynomial $f(x) \in \mathbb{R}[x]$ such that $f(u) = 0$. This will imply $u \in \mathbb{C}$—that is $\mathbb{C}$ is algebraically closed
The field extensions of $\mathbb{C}$,

$$\mathbb{C} \rightarrow \mathbb{F}$$

have the property

- If $u \in \mathbb{F}$ satisfies an equation

$$f(u) = 0,$$

$$u \in \mathbb{C}$$

- Otherwise $u$ said to be transcendental over $\mathbb{C}$. This is the case for every nonconstant

$$u = \frac{f(x)}{g(x)} \in \mathbb{C}(x)$$
Hilbert Nullstellensatz

**Theorem**

If the ideal \( I \subset R = \mathbb{C}[x_1, \ldots, x_n] \) is proper, i.e. \( I \neq R \), then \( V(I) \neq \emptyset \)—that is, if \( I \neq R \), there is \( c \) such that \( f(c) = 0 \) for all \( f \in I \).

**Proof.** We make two reductions.

1. Let \( m \) be a maximal ideal of \( R \) containing \( I \). Since \( V(m) \subset V(I) \), ETA that \( I \) is maximal.

2. Indeed, if \( c \in \mathbb{C}^n \) is such that \( f(c) = 0 \) for all \( f(x) \in m \), then \( g(c) = 0 \) for all \( g \in I \subset m \).
Nullstellensatz

After these reductions the assertion is:

**Theorem**

*If $M$ is a maximal ideal of $R = \mathbb{C}[x_1, \ldots, x_n]$, then there is*

$$c = (c_1, \ldots, c_n) \in \mathbb{C}^n$$

*such that*

$$f(c) = 0 \quad \forall f(x) \in M.$$
Special case: \( \mathbb{C} \)

Consider the field \( \mathbf{F} = \mathbb{C}[x_1, \ldots, x_n]/M. \)

**Proposition**

*It is ETS that \( \mathbf{F} \) is isomorphic to \( \mathbb{C} \).*

**Proof.** Indeed, if \( \mathbf{F} \cong \mathbb{C} \), for each indeterminate \( x_i \) its equivalence class in \( \mathbb{C}[x_1, \ldots, x_n]/M \) contains some element \( c_i \) of \( \mathbb{C} \), that is \( x_i - c_i \in M. \) this means that

\[
(x_1 - c_1, \ldots, x_n - c_n) \subset M.
\]

But \( (x_1 - c_1, \ldots, x_n - c_n) \) is also a maximal ideal, therefore it is equal to \( M. \) Clearly every polynomial of \( M \) vanishes at \( c = (c_1, \ldots, c_n). \) \( \square \)
Proof of $\mathbb{C} = \mathbb{C}[x_1, \ldots, x_n]/M$

1. ETS that the extension $\mathbb{C} \rightarrow F = \mathbb{C}[x_1, \ldots, x_n]/M$ is algebraic.

2. Observe that $[F : \mathbb{C}]$, the dimension of $F$ as a vector space over $\mathbb{C}$, is countable, $F$ being a homomorphic image of the countably generated vector space $\mathbb{C}[x_1, \ldots, x_n]$.

3. If $F$ is not algebraic over $\mathbb{C}$, suppose $t \in F$ is transcendental over $\mathbb{C}$.

4. Consider the uncountable set $\{1/(t - c), c \in \mathbb{C}\}$. 
Since they cannot be linearly independent, there are distinct \( c_i \), \( 1 \leq i \leq m \) and nonzero \( r_i \in \mathbb{C} \) such that

\[
r_1 \frac{1}{t - c_1} + \cdots + r_m \frac{1}{t - c_m} = 0.
\]

Clearing denominators gives the equality of two polynomials of \( \mathbb{C}[t] \):

\[
r_1(t - c_2)(t - c_3) \cdots (t - c_m) = (t - c_1)g(t),
\]

which is a contradiction as the \( c_i \) are distinct.
Comaximal ideals

**Definition**

Two ideals $I$ and $J$ of a ring $R$ are **comaximal** if

$$I + J = R.$$ 

**Example**

$R = \mathbb{Z}$, $I = (6)$, $J = (35)$, then $I + J = \mathbb{Z}$. 

Partition of the Unity

If $R$ is a commutative ring, a partition of the unity is an special decomposition of the form

$$R = J_1 + \cdots + J_n, \quad J_i \text{ ideals of } R$$

Suppose $I_1, \ldots, I_n$ is a set of ideals that is pairwise co-maximal, meaning $I_i + I_j = R$, for $i \neq j$. This obviously is a partition of the unity.

Another arises from it [check!] if we set $J_i = \prod_{j \neq i} I_j$

$$R = J_1 + \cdots + J_n, \quad J_i \text{ ideals of } R$$
Chinese Remainder Theorem

Theorem
If \( I_i, i \leq n, \) is a family of ideals that is pairwise co-maximal, then for \( I = I_1 \cap I_2 \cap \cdots \cap I_n \) there is an isomorphism

\[
R/I \cong R/I_1 \times \cdots \times R/I_n.
\]

Proof. Set \( J_i = \prod_{j \neq i} I_j. \) Note that \( I_i + J_i = R. \) Since \( J_1 + \cdots + J_n = R, \) there is an equation

\[
1 = a_1 + \cdots + a_n, \quad a_i \in J_i
\]

Note that for each \( i, a_i \cong 1 \mod I_i. \) Define a mapping \( h \) from \( R \) to \( R/I_1 \times \cdots \times R/I_n, \) by \( h(x) = (xa_1, \ldots, xa_n). \) We claim that \( h \) is a surjective homomorphism of kernel \( I. \)
1. Since $a_i \equiv 1 \mod l_i$,

$$h(x) = (xa_1, \ldots, xa_n) = (\bar{x}_1, \ldots, \bar{x}_n)$$

which is clearly a homomorphism.

2. The kernel consists of the $x$ such that $\bar{x}_i = 0$ for each $i$, that is $x \in l_i$ for each $i$—that is, $x \in l$.

3. To prove $h$ surjective, for $u = (\bar{x}_1, \ldots, \bar{x}_n)$, setting

$$x = x_1 a_1 + \cdots + x_n a_n$$

gives $h(x) = u$. 
Example

How ancient astronomers calculated 1°: That is, how to divide the circle by 360.

- $360 = 8 \times 9 \times 5$: primary decomposition.
- The numbers 72, 40 and 45 have no common factor, so form a partition of the 1:

$$1 = 5 \times 45 - 2 \times 72 - 2 \times 40$$

$$\frac{1}{360} = \frac{5}{8} - \frac{2}{5} - \frac{2}{9}$$
GCD of polynomials

If $f(x)$ and $g(x)$ are polynomials in $F[x]$, the **greatest common divisor** is the monic polynomial of highest degree $h(x)$ that divides $f(x)$ and $g(x)$

$$\gcd(f(x), g(x)) = h(x)$$

For example,

$$\gcd((x - 1)^3(x - 2)^2, (x - 1)(x - 2)^4) = (x - 1)(x - 2)^2.$$  

An elementary, but very useful fact, is that **long division** provides an effective method to find gcds.
Proposition

A polynomial $f(x) \in \mathbb{R}[x]$ of degree $f(x) \geq 1$ has multiple roots if and only if $\gcd(f(x), f'(x)) \neq 1$.

Thus, while it is hard to find the roots of a polynomial $f(x)$, it is easy to determine whether it has multiple roots!

The explanation is very simple: If $f(x)$ has a root of algebraic multiplicity $m$,

$$f(x) = (x - a)^m g(x), \quad g(a) \neq 0,$$

its derivative

$$f'(x) = m(x - a)^{m-1} g(x) + (x - a)^m g'(x)$$

has $a$ as a root with multiplicity $m - 1$. This implies that $(x - a)^{m-1}$ is a common factor of $f(x)$ and $f'(x)$, and therefore will be a factor of $\gcd(f(x), f'(x))$. 
If \( \gcd(f(x), f'(x)) = 1 \), then \( f(x) \) has no repeated (complex) roots.

Suppose \( f(x) \) is the characteristic polynomial of a 3-by-3 complex matrix \( A \), and we must decide whether it is diagonalizable. What to do?

1. If \( \gcd(f(x), f'(x)) = 1 \), by the discussion above the roots are distinct, and we are done: \( A \) is diagonalizable.

2. If there is a double root \( a \) and a single root \( b \), \( \gcd(f(x), f'(x)) = (x - a) \). We check the dimension of the eigenspace \( E_a \), if \( \dim E_a = 2 \), ok, otherwise not diagonalizable.

3. If \( a \) is a triple root, \( \gcd(f(x), f'(x)) = (x - a)^2 \). Again we check whether \( \dim E_a = 3 \).
Recall the long division algorithm for polynomials in $\mathbb{F}[x]$: If $f(x), g(x) \neq 0$ are polynomials, there exist polynomials $q(x), r(x)$ such that

$$f(x) = q(x)g(x) + r(x), \quad r(x) = 0 \text{ or } \deg r(x) < \deg g(x)$$

Look at a consequence:

$$\gcd(f(x), g(x)) = \gcd(g(x), r(x))$$

since any polynomial $p(x)$ that divides (both) $f(x), g(x)$ will divide $g(x), r(x)$, and conversely. Note that the data of $g(x), r(x)$ has lower degrees, so we can turn this into an algorithm:
Starting at

\[ f(x) = q(x)g(x) + r(x), \]

1. Iterating, if \( r(x) \neq 0 \) and we divide
   \[ g(x) = q_1(x)r(x) + r_1(x), \]
   then any polynomial \( p(x) \) that divides (both) \( f(x), g(x) \) will divide \( r(x), r_1(x) \), and conversely.

2. Since \( \deg g(x) > \deg r(x) > \deg r_1(x) > \cdots \), ultimately we shall have
   \( r_{n-1}(x) = q_{n-1}(x)r_n(x), \quad r_n(x) \neq O. \)

3. \( r_n(x) \) is (a) largest degree polynomial that divides both \( f(x) \) and \( g(x) \), and any such polynomial will divide \( r_n(x) \).
Theorem

If \( r_n(x) \) is the last nonzero remainder in the sequence of long divisions, then \( r_n(x) \) divides \( f(x) \) and \( g(x) \). Moreover, there exist polynomials \( a(x), b(x) \) such that

\[
r_n(x) = a(x)f(x) + b(x)g(x).
\]

\( r_n(x) \) is called the (a) \textbf{GCD} of \( f(x) \) and \( g(x) \).

Proof: For simplicity suppose \( n = 2 \), so we have the divisions

\[
f = qg + r, \quad g = q_1 r + r_1, \quad r = q_2 r_1 + r_2, \quad r_1 = q_3 r_2
\]

\[
r_2 = r - q_2 r_1 = r - q_2(g - q_1 r) = r(1 + q_2 q_1) - q_2 g
\]

\[
= (f - qg)(1 + q_2 q_1) - q_2 g
\]

Now we collect the coefficient of \( f \)–it will be \( a(x) \)–and of \( g \)–it will be \( b(x) \): \( \gcd(f, g) = a(x)f(x) + b(x)g(x) \).
We are now going to apply these observations to the characteristic polynomial $p(x) = \det(A - xI)$ of a matrix $A$, whose eigenvalues $\lambda_i$ exist in the field $F$. Note for $F = \mathbb{C}$, this is the case for all matrices.

Underlying the following discussion is the assumption that

$$p(x) = \pm \prod_{i=1}^{m} (x - \lambda_i)^{m_i}.$$
1. If \( f(x) = (x - \lambda)^m \), \( g(x) = (x - \mu)^n \) and \( \lambda \neq \mu \) are different scalars, then \( \gcd(f(x), g(x)) = 1 \), this means that there is a (decomposition) \( 1 = a(x)f(x) + b(x)g(x) \).

2. Consider now the case of the 3 polynomials,

\[
f(x) = (x - \lambda_1)^m(x - \lambda_2)^n, \quad g(x) = (x - \lambda_1)^m(x - \lambda_3)^p, \quad h(x) = (x - \lambda_2)^n(x - \lambda_3)^p,
\]

where \( \lambda_1, \lambda_2, \lambda_3 \) are distinct. Note that

\[
\begin{align*}
\gcd(f, g) & = (x - \lambda_1)^m \\
\gcd(f, h) & = (x - \lambda_2)^n \\
\gcd(g, h) & = (x - \lambda_3)^p \\
\gcd(f, g, h) & = \gcd((x - \lambda_1)^m, h) = 1
\end{align*}
\]

3. These equations will imply that we have an equality

\[
1 = a(x)f(x) + b(x)g(x) + c(x)h(x).
\]
Suppose the characteristic polynomial of $T$ has a decomposition

$$\det(xI - T) = (x - a)^m(x - b)^n(x - c)^p.$$ 

The polynomials $f(x) = (x - b)^n(x - c)^p$, $g(x) = (x - a)^m(x - c)^p$, $h(x) = (x - a)^m(x - b)^n$, have $\gcd = 1$ as they have no common divisor. According to the observation above, we have an equality

$$1 = A(x)f(x) + B(x)g(x) + C(x)h(x)$$

Evaluating $x \rightarrow T$ gives the equality

$$\mathbf{1} = A(T)f(T) + B(T)g(T) + C(T)h(T)$$
Applying to an arbitrary vector \( \mathbf{v} \) we have

\[
\mathbf{v} = \mathbf{l}(\mathbf{v}) = A(T)(T - bl)^n(T - cl)^p(\mathbf{v}) + B(T)(T - al)^m(T - cl)^p(\mathbf{v}) \tag{v_1} + C(T)(T - al)^m(T - bl)^n(\mathbf{v}) \tag{v_3}
\]

\[
\mathbf{V} = \mathbf{v}_1 + \mathbf{v}_2 + \mathbf{v}_3
\]

\[
(T-al)^m(\mathbf{v}_1) = A(T)(T-al)^m(\mathbf{v}_1) = A(T)(T-al)^m(T-bl)^n(T-cl)^p(\mathbf{v}) = 0
\]

by Cayley-Hamilton. This says that every vector \( \mathbf{v} \) is a sum of vectors in \( K_a, K_b \) and \( K_c \). It is also easy to see that \( \mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3 \) are linearly independent.
Chinese Remainder Theorem

**Theorem**

Let \( f_1(x), \ldots, f_m(x) \) be polynomials of \( \mathbb{F}[x] \). If \( g(x) = \gcd(f_1(x), \ldots, f_m(x)) \) there are polynomials \( a_i(x) \) such that

\[
g(x) = a_1(x)f_1(x) + \cdots + a_m(x)f_m(x).
\]

Let \( T \) be a linear operator on the finite-dimensional vector space \( V \). Suppose its characteristic polynomial \( \det(T - xI) \) splits:

\[
f(x) = \pm \prod_{i=1}^{m} (x - \lambda_i)^{n_i}, \quad \text{distinct } \lambda_i.
\]

For each \( i \), setting \( f_i(x) = \frac{f(x)}{(x-\lambda_i)^{n_i}} \), gives us a collection \( f_1(x), \ldots, f_m(x) \) of \( \gcd = 1 \): In

\[
1 = a_1(x)f_1(x) + \cdots + a_m(x)f_m(x)
\]

\[
\text{replace } x \rightarrow T
\]
\[ I = a_1(T)f_1(T) + \cdots + a_m(T)f_m(T) \]

Now we are going to make several observations about this decomposition.

1. The range of \( f_i(T) \) is contained in the generalized eigenspace \( K_{\lambda_i} \): If \( u = f_i(T)(v) \),

\[
(T - \lambda_i)^{n_i}f_i(T)(v) = f(T)(v) = 0,
\]

since by the Cayley-Hamilton theorem \( f(T) = 0 \).

2. For every \( v \in V \)

\[
v = I(v) = \underbrace{a_1(T)f_1(T)(v)}_{\in K_{\lambda_1}} + \cdots + \underbrace{a_m(T)f_m(T)(v)}_{\in K_{\lambda_m}}
\]
Generalized eigenvectors and eigenspaces

- If $T$ is a linear operator of the vector space $V$ and $\lambda$ is a scalar, a nonzero vector $v \in V$ is a **generalized eigenvector** of $T$ if $(T - \lambda I)^p(v) = O$ for some positive integer $p$. We denote this set, together with the vector $O$, by $K_\lambda$. $K_\lambda$ is usually bigger than the eigenspace $E_\lambda$.

- In fact,

$$V = \bigoplus_i K_{\lambda_i},$$

in particular, $V$ has a basis made up of generalized eigenvectors.
This representation says that every vector \( \mathbf{v} \in \mathbf{V} \) can be written as

\[
\mathbf{v} = \mathbf{v}_1 + \cdots + \mathbf{v}_m, \quad \mathbf{v}_i \in K_{\lambda_i}
\]

Since we already proved that \( \dim K_{\lambda_i} \leq n_i \), the algebraic multiplicity of \( \lambda_i \), this equality proves equality of the dimensions. It can be written as

\[
\mathbf{V} = K_{\lambda_1} \oplus \cdots \oplus K_{\lambda_m},
\]

and the matrix representation of \( \mathbf{T} \) has the block format (after picking bases of the \( K_{\lambda_i} \)'s)

\[
[\mathbf{T}] = \begin{bmatrix}
[\mathbf{T}]_1 & \cdots & \mathbf{O} \\
\vdots & \ddots & \vdots \\
\mathbf{O} & \cdots & [\mathbf{T}]_m
\end{bmatrix}
\]
What this does is to allow us to assume that the characteristic polynomial of $T$ has the form $(x - \lambda)^n$. We will argue that such linear operator have a matrix representation made up of Jordan blocks with the same $\lambda$. Let us look at one such $p \times p$ block

$$A = [v_1 | \cdots | v_p] = \begin{bmatrix}
\lambda & 1 & 0 & \cdots & 0 & 0 \\
0 & \lambda & 1 & \cdots & 0 & 0 \\
\vdots & \vdots & \ddots & \ddots & \vdots & \vdots \\
0 & 0 & 0 & \cdots & \lambda & 1 \\
0 & 0 & 0 & \cdots & 0 & \lambda
\end{bmatrix}$$

$A(v_1) = \lambda v_1$, $A(v_2) = v_1 + \lambda v_2$, $\cdots$, $A(v_p) = v_p - 1 + \lambda v_p$

If we write these equations in the reverse order, we get
\((A - \lambda I)(v_p) = v_{p-1}\)
\[(A - \lambda I)^2(v_p) = v_{p-2}\]
\[\vdots\]
\[(A - \lambda I)^{p-1}(v_p) = v_1\]
\[(A - \lambda I)^p(v_p) = 0\]

Starting on \(v_p\) and applying \(U = A - \lambda I\) repeatedly we get all the vectors of the basis

\[v_p \rightarrow v_{p-1} \rightarrow \cdots \rightarrow v_2 \rightarrow v_1 \rightarrow 0\]

We will say that \(v_p\) is the generator of the basis, and that \(\gamma = \{v_1, v_2, \ldots, v_p\}\) is a cycle of generalized eigenvectors, \(v_1\) is the initial and \(v_p\) the end vectors: They form a so-called dot diagram
Proposition

Let $T$ be a linear operator on the vector space $V$. For some scalar $\lambda$ and some integer $p$, suppose $v$ is a nonzero vector such that

$$(T - \lambda I)^p(v) = O, \quad (T - \lambda I)^{p-1}(v) \neq O.$$  

Then the $p$ vectors $(T - \lambda I)^{p-1}(v), \ldots, (T - \lambda I)(v), v$ are linearly independent. They span a $T$-invariant subspace $W$ and the matrix representation of $[T]_W$ with respect to this basis is a Jordan block.

Proof: Let us denote these vectors by $v_1, \ldots, v_p = v$, respectively. Suppose we have a linear relation

$c_1 v_1 + \cdots + c_p v_p = O$. Let us prove all $c_i = 0$. Let us argue just one case as the general case is similar. Suppose $c_p \neq 0$. Apply the operator $(T - \lambda I)^{p-1}$ to the relation to obtain
\[ v_i = (T - \lambda I)^{p-i}(v) \]
\[ c_1(T - \lambda I)^{p-1}(v_1) + \cdots + c_p \underbrace{(T - \lambda I)^{p-1}(v_p)}_{=v_1} = O \]

Note that all terms vanish, except for the last. This contradicts \( c_p \neq 0 \).

The subspace \( W \) clearly satisfies \( T(W) \subset W \). Finally, note that

\[
T(v_i) = T(T - \lambda I)^{p-i}(v) = (T - \lambda I)^{p-i+1}(v) + \lambda(T - \lambda I)^{p-i}(v) = v_{i-1} + \lambda v_i,
\]
which shows that the matrix representation is

\[
\begin{bmatrix}
\lambda & 1 & \cdots & 0 \\
\vdots & \vdots & \ddots & \vdots \\
0 & 0 & \cdots & 1 \\
0 & 0 & \cdots & \lambda
\end{bmatrix}
\]
We come now to the crux of the problem: Given a linear operator $T$ whose characteristic polynomial is $\pm(x - \lambda)^n$, to prove that there is a matrix representation made up of $\lambda$-Jordan blocks (same $\lambda$)

\[
\begin{bmatrix}
J_1 & O & O \\
O & J_2 & O \\
O & O & J_3
\end{bmatrix}
= \begin{bmatrix}
\lambda & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & \lambda & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & \lambda & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & \lambda & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & \lambda & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & \lambda & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & \lambda & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & \lambda
\end{bmatrix}
\]

We are going to prove the existence of such representation and the uniqueness of the number and sizes of the blocks.
Situation:

\( T : K_\lambda \to K_\lambda, \dim K_\lambda = n, \) characteristic polynomial of \( T \) is \((x - \lambda)^n\). The eigenspace is \( E_\lambda \subset K_\lambda \).

**Goal:** We will show that \( K_\lambda \) has a basis

\[
B = \bigcup_{i=1}^{m} \gamma_i
\]

where each \( \gamma_i \) is a cycle of generalized eigenvectors. The Jordan representation comes from the corresponding matrix representation. For example, if \( K_\lambda = E_\lambda \), then a basis of \( E_\lambda \) gives the cycles, all of length 1, and the matrix representation is just \( \lambda I_n \).
We are going to argue by induction on \( n = \dim K_\lambda \). If \( n = 1 \) (or, more generally, \( K_\lambda = E_\lambda \)), there is nothing to prove.

Let \( Z \) be the range of \( T - \lambda I \). For simplicity of notation call this map \( U : K_\lambda \to K_\lambda \). Note that \( E_\lambda \) is the nullspace of \( U \), and therefore \( \dim E_\lambda + \dim Z = n \), by the dimension formula.

Since \( \dim Z < n \) and the characteristic polynomial of the restriction of \( T \) to \( Z \) divides \((x - \lambda)^n\), the induction hypothesis guarantees a basis for \( Z \):

\[ \gamma' : w, (T - \lambda I)(w), \ldots, (T - \lambda I)^{p-1}(w) \]

\[ \mathcal{B}' = \bigcup_{i=1}^{r} \gamma_i' \]

where each \( \gamma_i' \) is a cycle of generalized eigenvectors of \( Z \). Let us consider one of these cycles \( \gamma' \):
\[ \gamma_i': \; w, (T - \lambda I)(w), \ldots, (T - \lambda I)^{p-1}(w) \]

But \( w \) belongs to the range of \((T - \lambda I)\), that is \( w = (T - \lambda I)(v) \), for some \( v \in V \). This gives a cycle of \( V \) itself:

\[ \gamma_i : v, (T - \lambda I)(v), \ldots, (T - \lambda I)^p(v) \]

In this manner, for every \( \gamma_i' \) of \( Z \) we get a longer cycle (by 1 more vector) of \( V \).

We recall that vector at the end of the list are the only eigenvectors and that

\[
\bigcup_{i=1}^{r} \gamma_i
\]

contains just \( r \) independent eigenvectors, the same set as the basis \( B' \) of \( Z \). If these eigenvectors are \( u_1, \ldots, u_r \), add (if necessary) \( u_{r+1}, \ldots, u_s \) to form a basis of the eigenspace \( E_\lambda \). Each of these \( u_i \) defines a new cycle \( \gamma_i \) of length 1, \( i > r \).
Dot Diagrams and Enlarged Cycles

•: vectors in the set $B'$
•: vectors added.

$T - \lambda I$ maps each dot to dot under. Last row is a basis of $E_\lambda$: it is mapped to $O$. 
Proposition (Very technical, I apologize)

The vectors in the set

\[ \mathcal{B} = \bigcup_{i=1}^{s} \gamma_i \]

form a basis of \( V \).

Proof: First let us count the number of elements of added to pass from the basis \( \mathcal{B}' \) of \( Z \) to the set \( \mathcal{B} \) of \( V \):

\[ r \ (1 \text{ for each of the } r \text{ cycles in } \mathcal{B}') + (s - r) = s = \dim E_\lambda \]

Therefore \( \text{cardinality of } \mathcal{B}' + s = \dim Z + s = n = \dim V \)

To prove \( \mathcal{B} \) is a basis, ETS that it spans \( V \), as they have already the right number of elements for a basis.
Let \( u \in V \) and consider \((T - \lambda I)(u) \in Z\). Since every vector in \( B' \) is the image under \( T - \lambda I \) of some vector in \( B \), we can write

\[
(T - \lambda I)(v) = \text{Linear combination of } (T - \lambda I)(v_i), \quad v_i \in B.
\]

This implies that

\[
(T - \lambda I) \left( v - \text{Linear combination of } v_i \right) = O = w
\]

Thus \( w \in E_\lambda \). Since \( B \) contains a basis of \( E_\lambda \), this implies \( v \) lies in the span of \( B \).
To illustrate the uniqueness of Jordan decomposition, suppose $T$ gives rise to two different cycle decomposition for $K_\lambda$:

\[
\begin{array}{c}
\bullet \\
\bullet \\
\bullet \\
\bullet \\
\bullet
\end{array}
\quad \text{and} \quad 
\begin{array}{c}
\bullet \\
\bullet \\
\bullet \\
\bullet \\
\bullet \\
\bullet
\end{array}
\]

Observe that many things match: $\dim K_\lambda = 12$ [number of dots, red or black], $\dim E_\lambda = 5$ (number of piles, columns). Now we are going to observe things that are off:

\[(T - \lambda I)^4\text{(any } \bullet \text{)} = 0, \quad (T - \lambda I)^4\text{(top } \bullet \text{)} \neq 0\]
This illustrate the argument: The number of dots at level $\ell$ is the dimension of the subspace of the vectors $v$ of $V$ such that

$$(T - \lambda I)^\ell(v) = 0$$
Diagonalization and Minimal Polynomials

Let $S$ be the ring of $n \times n$ matrices and $A \in S$. We look at $A$ as a linear transformation $A : \mathbb{F}^n \rightarrow \mathbb{F}^n$. $S$ is a ring which as a $\mathbb{F}$-vector space has dimension $n^2$. Consider the ring homomorphism defined by the evaluation

$$\varphi : R = \mathbb{F}[x] \rightarrow S, \quad \varphi(x) = A$$

**Proposition**

$\ker \varphi \neq (0)$.

**Proof.**

$\varphi$ cannot be injective since it maps the infinite dimensional vector space $\mathbb{F}[x]$ into the finite dimensional vector space $S$. □
Minimal Polynomial

By the theorem about the ideals of $F[x]$, $\ker(\varphi) = (m(x))$. For convenience we pick $m(x)$ as monic. Thus, given a square matrix $A$, there are polynomials $f(x)$ such that

$$f(A) = 0.$$ 

The best known is $f(x) = \det(A - xI)$, the characteristic polynomial: by Cayley-Hamilton:

$$f(A) = 0.$$ 

What else?
**Definition**

Let $A$ be a $n$-by-$n$ matrix. The **minimal polynomial** of $A$ is the monic polynomial $m(x) = x^m + c_{m-1}x^{m-1} + \cdots + c_0$ of least degree such that

$$m(A) = A^m + c_{m-1}A^{m-1} + \cdots + c_0I = O.$$ 

1. If $A = I_n$, then $m(x) = x - 1$.
2. If $A = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$, $m(x) = x^2$.
3. In the case of [the Jordan block] $J = \begin{bmatrix} \lambda & 1 & 0 \\ 0 & \lambda & 1 \\ 0 & 0 & \lambda \end{bmatrix}$, 
   $$m(x) = (x - \lambda)^3.$$ 
   For a block of size $n$, $m(x) = (x - \lambda)^n$. 
\[ \mathbf{J} = \begin{bmatrix} \lambda & 1 & 0 & 0 \\ 0 & \lambda & 1 & 0 \\ 0 & 0 & \lambda & 1 \\ 0 & 0 & 0 & \lambda \end{bmatrix}, \quad \mathbf{U} = \mathbf{J} - \lambda \mathbf{I} = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix} \]

\[ \mathbf{U}^2 = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}, \quad \mathbf{U}^3 = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}, \quad \mathbf{U}^4 = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \]

\[ m(x) = (x - \lambda)^4 \]

Observe the right drift of the diagonal of 1’s until it leaves the matrix!
Corollary

The minimal polynomial $m(x)$ of $A$ divides the characteristic polynomial $p(x) = \det(A - xI)$ of $A$. In particular $\deg m(x) \leq n$. 
Diagonalization

**Theorem**

*A is diagonalizable if and only if its minimal polynomial \( m(x) \) has no repeated root.*

**Proof.** In the forward direction, the assertion is clear: If \( A \) is made up of diagonal blocks

\[
A = \begin{bmatrix}
\lambda_1 I_1 & 0 & \cdots & 0 \\
0 & \lambda_2 I_2 & \cdots & 0 \\
\vdots & \vdots & \ddots & 0 \\
0 & 0 & \cdots & \lambda_r I_r
\end{bmatrix},
\]

with \( \lambda_i \) distinct, its minimal polynomial is

\[
m(x) = \prod_{i=1}^{r} (x - \lambda_i)
\]
For the converse, suppose the characteristic polynomial of $T$ has a decomposition

$$\det(xI - T) = (x - a)^m(x - b)^n(x - c)^p.$$ 

The polynomials $f(x) = (x - b)^n(x - c)^p$, $g(x) = (x - a)^m(x - c)^p$, $h(x) = (x - a)^m(x - b)^n$, their gcd = 1 as they have no common divisor. According to earlier observations, above we have an equality

$$1 = A(x)f(x) + B(x)g(x) + C(x)h(x)$$

Evaluating $x \rightarrow T$ gives the equality

$$I = A(T)f(T) + B(T)g(T) + C(T)h(T)$$
Applying to an arbitrary vector $\mathbf{v}$ we have

$$
\mathbf{v} = \mathbf{I}(\mathbf{v}) = \underbrace{A(T)(T - bl)^n(T - cl)^p(\mathbf{v})}_{\mathbf{v}_1} + \underbrace{B(T)(T - al)^m(T - cl)^p(\mathbf{v})}_{\mathbf{v}_2} + \underbrace{C(T)(T - al)^m(T - bl)^n(\mathbf{v})}_{\mathbf{v}_3}
$$

$$
\mathbf{V} = \mathbf{v}_1 + \mathbf{v}_2 + \mathbf{v}_3
$$

$$(T - al)^m(\mathbf{v}_1) = A(T)(T - al)^m(\mathbf{v}_1) = A(T)(T - al)^m(T - bl)^n(T - cl)^p(\mathbf{v}) = 0$$

by Cayley-Hamilton. This says that every vector $\mathbf{v}$ is a sum of vectors in $K_a$, $K_b$ and $K_c$. It is also easy to see that $\mathbf{v}_1$, $\mathbf{v}_2$, $\mathbf{v}_3$ are linearly independent.
Now we are going to make several observations about this decomposition.

1. The range of $f_i(T)$ is contained in the generalized eigenspace $K_{\lambda_i}$: If $u = f_i(T)(v)$,

$$
(T - \lambda_i)^{n_i} f_i(T)(v) = f(T)(v) = 0,
$$

since by the Cayley-Hamilton theorem $f(T) = 0$.

2. For every $v \in V$

$$
v = I(v) = \underbrace{a_1(T)f_1(T)(v)}_{\in K_{\lambda_1}} + \cdots + \underbrace{a_m(T)f_m(T)(v)}_{\in K_{\lambda_m}}
$$
Generalized eigenvectors and eigenspaces

- If $T$ is a linear operator of the vector space $V$ and $\lambda$ is a scalar, a nonzero vector $v \in V$ is a **generalized eigenvector** of $T$ if $(T - \lambda I)^p(v) = 0$ for some positive integer $p$. We denote this set, together with the vector $0$, by $K_\lambda$. $K_\lambda$ is usually bigger than the eigenspace $E_\lambda$.
- In fact, 
  \[ V = \bigoplus_{i} K_{\lambda_i}, \]
  in particular, $V$ has a basis made up of generalized eigenvectors.
This representation says that every vector \( \mathbf{v} \in \mathbf{V} \) can be written as
\[
\mathbf{v} = \mathbf{v}_1 + \cdots + \mathbf{v}_m, \quad \mathbf{v}_i \in K_{\lambda_i}
\]
Since we already proved that \( \dim K_{\lambda_i} \leq n_i \), the algebraic multiplicity of \( \lambda_i \), this equality proves equality of the dimensions. It can be written as
\[
\mathbf{V} = K_{\lambda_1} \oplus \cdots \oplus K_{\lambda_m},
\]
and the matrix representation of \( \mathbf{T} \) has the block format (after picking bases of the \( K_{\lambda_i} \)'s)
\[
[T] = \begin{bmatrix}
[T]_1 & \cdots & O \\
\vdots & \ddots & \vdots \\
O & \cdots & [T]_m
\end{bmatrix}
\]
Conclusion:

- This block decomposition says that the minimal polynomial $f(x)$ of $T$ is the product of the minimal polynomials of the restrictions on $K_{\lambda_i}$

$$f(x) = p_1(x) \cdots p_m(x)$$

- If some $T_i$ is not diagonalizable, its minimal polynomial has a factor $(x - a)^2$, and $f(x)$ will have some multiple root.
Group Representations

**Theorem**

Let $G$ be a finite subgroup of $GL_n(\mathbb{C})$. Then any element $A \in G$ is diagonalizable.

**Proof.**

- Since $G$ is finite, $A$ has finite order, that is $A^r = I$ for some integer $r$.
- This implies that $x^r - 1$ lies in the ideal $(m(x))$ generated by the minimal polynomial of $A$, and therefore $x^r - 1 = m(x)p(x)$.
- It follows that every root of $m(x)$ is a root of $x^r - 1$. But the roots of $x^r - 1$ are distinct (the derivative is $rx^{r-1}$, whose roots are zero). Therefore the roots of $m(x)$ are distinct.
Corollary

If $G$ is a finite subgroup of $GL_n(\mathbb{C})$, then the order of every element $A \in G$ is at most $n$. 
Homework #11

Do 5 Problems.

1. Prove that the kernel of the homomorphism $\varphi : \mathbb{C}[x, y] \to \mathbb{C}[t]$ defined by $x \mapsto t^2$, $y \mapsto t^3$ is the principal ideal generated by $x^3 - y^2$.

2. The nilradical $N$ of a ring $R$ is the set of nilpotent elements. Prove that $N$ is an ideal. Find $N$ when $R = \mathbb{Z}_{72}$.

3. Prove that $\mathbb{Z}[i]/(i + 2)$ is isomorphic to $\mathbb{Z}/(m)$ for some $m$. Determine $m$.

4. Determine the maximal ideals of $\mathbb{R}[x]/(x^2 - 3x + 2)$.

5. Prove that the ring $\mathbb{Z}_2[x]/(x^3 + x + 1)$ is a field but $\mathbb{Z}_3[x]/[x^3 + x + 1]$ is not.

6. Find an isomorphic direct product of cyclic groups for the group:
V is generated by the elements \( x, y, z \);

These elements satisfy the relations

\[
\begin{align*}
7x + 5y + 2z &= 0, \\
3x + 3y &= 0, \\
13x + 11y + 2z &= 0.
\end{align*}
\]