Math 552: Abstract Algebra II

Wolmer V. Vasconcelos

Set 2

Spring 2009
Outline

1. Rings and Modules
2. Chain Conditions
3. Assignment #6
4. Prime Ideals
5. Assignment #7
6. Primary Decomposition
7. Intro Noetherian Rings
8. Assignment #8
9. Homework
10. Modules of Fractions
11. Assignment #9
12. Integral Extensions
13. Integral Morphisms
14. Assignment #10
15. TakeHome #1
Composition laws

A composition on a set $X$ is a function assigning to pairs of elements of $X$ an element of $X$,

$$(a, b) \mapsto f(a, b).$$

That is a function of two variables on $X$ with values in $X$. It is nicely represented in a composition table

$$
\begin{array}{c|c|c|c}
  f & * & b & * \\
  * & * & * & * \\
  a & * & f(a, b) & * \\
  * & * & * & * \\
\end{array}
$$

We represent it also as

$$X \times X \xrightarrow{f} X$$
Example: Abelian group

An abelian group is a set $G$ with a composition law denoted ‘$+$’

$$G \times G \to G,$$

$$a, b \in G, \quad a + b \in G$$

satisfying the axioms

- **associative** $\forall a, b, c \in G, \quad (a + b) + c = a + (b + c)$
- **commutative** $\forall a, b \in G, \quad a + b = b + a$
- **existence of $O$**
  $$\exists O \in G \quad \text{such that } \forall a \quad a + O = a$$

- **existence of inverses**
  $$\forall a \in G \quad \exists b \in G \quad \text{such that } a + b = O$$

This element is unique and denoted $-a$. 
Rings

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:

\[
e = ee' = e'e = e'
\]
A ring $R$ is a set with two composition laws $+$ and $\times$ satisfying

- $\{R, +\}$ is an abelian group
- **associative axiom**: For $a, b, c \in R$,
  \[ a \times (b \times c) = (a \times b) \times c \]
- **distributive axioms**: For $a, b, c \in R$,
  \[ a \times (b + c) = a \times b + a \times c \quad \text{and} \quad (a + b) \times c = a \times c + b \times c \]
- **existence of 1**: there is $e \in R$ such that for $a \in R$,
  \[ a \times e = e \times a = a \]
- If $a \times b = b \times a$ for all $a, b \in R$, ring is called **commutative**
Class Surprise Quiz!

What is your favorite ring?

To qualify, your answer must be different—very different—from that given by a classmate!
More composition laws

Other composition laws take pairs [or triples,...] of sets: such as a function assigning to pairs of elements of $Y$ and $X$ an element of $X$,

$$(a, b) \mapsto f(a, b).$$

It is represented in a composition table

<table>
<thead>
<tr>
<th></th>
<th>$*$</th>
<th>$b$</th>
<th>$*$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$*$</td>
<td>$*$</td>
<td>$*$</td>
<td>$*$</td>
</tr>
<tr>
<td>$a$</td>
<td>$*$</td>
<td>$f(a, b)$</td>
<td>$*$</td>
</tr>
<tr>
<td>$*$</td>
<td>$*$</td>
<td>$*$</td>
<td>$*$</td>
</tr>
</tbody>
</table>

We represent it also as $Y \times X \xrightarrow{f} X$

Typically we place requirements on $f$, such as $f(a, b + c) = f(a, b) + f(a, c)$
If $R$ is a ring, a **left $R$-module** $M$ is a set

- $\{M, +\}$ is an abelian group and equipped with a mapping $(R, M) \rightarrow M$, $(a, m) \rightarrow am$ such that
- **associative axiom**: For $a, b \in R$, $c \in M$, $a(bc) = (a \times b)c$
- **distributive axiom**: For $a \in R$, $b, c \in M$, $a(b + c) = ab + ac$
- If 1 is the identity of $R$, $1c = c$ for all $c \in M$
Submodules, quotient modules, homomorphisms

- If $R$ is a ring and $A$ and $B$ are left $R$-modules, a group homomorphism $f : A \rightarrow B$ is a $R$-homomorphism if

  $$f(ax) = af(x), \quad a \in R, \quad x \in A.$$ 

- A subgroup $C$ of the $R$-module $A$ is a submodule if the inclusion mapping $C \rightarrow A$ is a homomorphism. If $C$ is a submodule, the quotient group $A/C$ is an $R$-module.

- If $f : A \rightarrow B$ is a homomorphism of $R$-modules, $K = \ker (f) = \{x \in A : f(x) = 0\}$ is a submodule of $A$, and $E = \{f(a) : a \in A\}$ is a submodule of $B$.

- There is a canonical isomorphism of $R$-modules $A/K \cong E$.
Direct sums and products

Let $R$ be a ring and $\{M_\alpha : \alpha \in I\}$ be a family of modules.

- **direct sum** $M = \bigoplus_\alpha M_\alpha$ is the set of $(m_\alpha : \alpha \in I)$, almost all $m_\alpha = 0_\alpha$. Addition and multiplication by elements of $R$ is component wise, for instance

  $$ (m_\alpha) + (n_\alpha) = (m_\alpha + n_\alpha) $$

- **direct product** $M = \prod_\alpha M_\alpha$ is the set of $(m_\alpha : \alpha \in I)$. Addition and multiplication by elements of $R$ is component wise, for instance

  $$ a(m_\alpha) = (am_\alpha) $$
Generators of a module

- If $A$ is an $R$-module, a subset $S \subseteq A$ is a set of generators of $A$ if for $a \in A$ there are $s_1, \ldots, s_n$ in $S$ and $r_i \in R$ such that

\[ a = r_1 s_1 + \cdots + r_n s_n \]

- If $S$ is finite, $A$ is said to be **finitely generated**
- If $S = \{s\}$, $A$ is said to be **cyclic**
Free modules

Let $R$ be a ring and $X$ a set. The free $R$-module with basis indexed by $X$:

$$F_X = \bigoplus_{x \in X} R_x, \quad R_x \simeq R$$

If $X = \{1, 2, \ldots, n\}$,

$$R^n = \{(a_1, \ldots, a_n), \quad a_i \in R\}$$

Set $e_1 = (1, 0, \ldots, 0), \ldots, e_n = (0, 0, \ldots, 1)$,

$$(a_1, a_2, \ldots, a_n) = a_1 e_1 + \cdots + a_n e_n$$
Finitely generated module

Proposition

Let $X$ be a set and $A$ an $R$-module. For any (set) mapping $\varphi : X \rightarrow A$ there is a (unique) module homomorphism

$$f : F_X = \bigoplus_{x \in X} Re_x \rightarrow A$$

such that $f(e_x) = \varphi(x)$.

Proposition

An $R$-module $A$ is finitely generated iff there is a surjection

$$f : R^n \rightarrow A,$$

for some $n \in \mathbb{N}$. 
Chain Conditions

Let $R$ be a ring and let $M$ be a left (right) $R$-module and denote by $X$ the set of $R$-submodules of $M$ ordered by inclusion.

A chain of submodules is a sequence

$$A_1 \subseteq A_2 \subseteq \cdots \subseteq A_n \subseteq \cdots$$

or

$$B_1 \supseteq B_2 \supseteq \cdots \supseteq B_n \supseteq \cdots$$

The first is called ascending, the other descending.
Noetherian Module

**Definition**

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

\( R \) is a left (right) **Noetherian** (Artinian) ring if the ascending (descending) chains of left (right) ideals are stationary.
Example

\[
\begin{bmatrix}
\mathbb{Z} & \mathbb{Q} \\
0 & \mathbb{Q}
\end{bmatrix}
\]

is a right (but not left) Noetherian ring.

\[
\begin{bmatrix}
\mathbb{Q} & \mathbb{R} \\
0 & \mathbb{R}
\end{bmatrix}
\]

is a left (but not right) Artinian ring.
Example: Sides may matter

Here is an example (J. Dieudonné) of a left Noetherian that is not right Noetherian.

Let \( A \) be the ring generated by \( x \) and \( y \), \( \mathbb{Z}[x, y] \), such that \( yx = 0 \) and \( yy = 0 \), and let \( R \) be the subring \( \mathbb{Z}[x] \). That is, \( R \) is the ring of polynomials in \( x \) over \( \mathbb{Z} \) (therefore \( R \) is Noetherian). \( A \) is the \( R \)-module

\[
A = R + Ry
\]

in particular \( A \) is a Noetherian left \( R \)-module, thus it is a left Noetherian ring.

Let \( I \) be the subgroup of \( A \) generated by \( \{x^n y, n \geq 0\} \). Since \( Ix = Iy = 0 \), \( I \) is a right ideal and thus any system of right \( R \)-generators of \( I \) is also a system of \( \mathbb{Z} \) generators. But \( I \) is not finitely generated over \( \mathbb{Z} \).
Maximal/Minimal Condition

**Definition**

\( M \) is an \( R \)-module with the Maximal Condition (Minimal Condition) if every subset \( S \) of \( X \) (set of submodules ordered by inclusion) contains a maximum submodule (minimum submodule).

**Proposition**

Let \( M \) be an \( R \)-module. Then

1. \( M \) is Noetherian iff \( M \) has the Maximal Condition.
2. \( M \) is Artinian iff \( M \) has the Minimal Condition.
Proof

Let $S$ be a set of submodules of $M$. If $S$ contains no maximal element, we can build an ascending chain

$$A_1 \subsetneq A_2 \subsetneq \cdots \subsetneq A_n \subsetneq \cdots$$

contradicting the assumption that $M$ is Noetherian. The converse has a similar proof.

Example: If $R = \mathbb{Z}$, $\mathbb{Z}$ is a Noetherian module, while for every prime number $p$, $\mathbb{Z}_{p^\infty}/\mathbb{Z}$ is Artinian.
Composition Series

**Proposition**

Let $M$ be an $R$-module satisfying both chain conditions. Then there exists a chain of submodules

$$0 \subset M_1 \subset M_2 \subset \cdots \subset M_{n-1} \subset M_n = M$$

such that each factor $M_i/M_{i-1}$ is a simple module.

Such sequences are called *composition series* of length $n$. The existence of one such series is equivalent to $M$ being both Noetherian and Artinian.

**Theorem (Jordan-Holder)**

All composition series of a module $M$ have the same length (called the *length* of $M$ and denoted $\lambda(M)$).
Noetherian Module

**Proposition**

*M is a Noetherian R-module iff every submodule is finitely generated.*

**Proof.**

Suppose *M* is Noetherian. Let us deny. Let *A* be a submodule of *M* 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 submodules, let \(B = \bigcup_{i \geq 1} A_i\) is a submodule and therefore \(B = (b_1, \ldots, b_m)\). Each \(b_i \in A_{n_i}\) for some \(n_i\). If \(n = \max\{n_i\}\), \(A_n = A_{n+1} = \cdots\).
Proposition

Let $R$ be a ring and

$$0 \rightarrow A \xrightarrow{f} B \xrightarrow{g} C \rightarrow 0$$

be a short exact sequence of $R$-modules (that is, $f$ is 1-1, $g$ is onto and $\text{Image } f = \ker g$). Then $B$ is Noetherian (Artinian) iff $A$ and $C$ are Noetherian (Artinian).
Corollary

If $R$ is a Noetherian (Artinian) ring, then any finitely generated $R$-module is Noetherian (Artinian).

Proof.

By the proposition, any f.g. free $R$-module $F = R \oplus \cdots \oplus R$ is Noetherian (Artinian). A f.g. $R$-module is a quotient of a f.g. free $R$-module.
Proof

Let $B_1 \subseteq B_2 \subseteq \cdots$ be an ascending sequence of submodules of $B$. Applying $g$ to it gives an ascending sequence $g(B_1) \subseteq g(B_2) \subseteq \cdots$ of submodules of $C$.

There is also an ascending sequence of submodules of $A$ by setting $A_i = f^{-1}(B_i)$.

There is $n$ such that both sequences are stationary from that point on: $g(B_n) = g(B_{n+1}) = \cdots$ and $f^{-1}(B_n) = f^{-1}(B_{n+1}) = \cdots$.

It follows easily that $B_n = B_{n+1} = \cdots$. 
Assignment #6

Define the following composition laws ($\oplus$ and $\otimes$) on the set $\mathbb{Z}$:

- For $a, b \in \mathbb{Z}$, set $a \oplus b := a + b + 1$
- For $a, b \in \mathbb{Z}$, set $a \otimes b := ab + a + b = (a + 1)(b + 1) - 1$

Call the integers with these two operations $\mathbb{Z}$ (read red integers). With proofs, answer the questions:

1. Is $\mathbb{Z}$ a ring?
2. If $\mathbb{Z}$ is a ring, is it isomorphic to $\mathbb{Z}$?
3. Define similarly $\mathbb{Q}$: is it a field?
4. List all that goes wrong.
5. Which generalizations occur to you?
Let us prove the following characterization of Noetherian modules over commutative rings:

**Definition**

Let $M$ be a module over the commutative ring $R$. The set $I$ of elements $x \in R$ such that $xm = 0$ for all $m \in M$ is an ideal called the **annihilator** of $M$, $I = \text{ann } M$.

**Proposition**

$M$ is a Noetherian module if and only if $M$ is finitely generated and $R/\text{ann } M$ is a Noetherian ring.
Hints

If a module $M$ is generated by $\{m_1, \ldots, m_n\}$ define the following mapping

$$f : R \longrightarrow M \oplus \cdots \oplus M, \quad f(r) = (rm_1, \ldots, rm_n)$$

verify that

- $f$ is a homomorphism, of kernel $\text{ann} M$
- Form the appropriate embedding of $R/\text{ann} M$ into the direct sum of the $M$'s to argue one direction
- Use, for the other direction, that $M$ is also a module over the ring $R/\text{ann} M$
Quotient rings

Let $I$ be a two-sided proper ideal of the $R$ and denote by $R/I$ the corresponding cosets $\{a + I : a \in R\}$.

The quotient ring $R/I$ is defined by the operations:

\[
(a + I) + (b + I) = (a + b) + I
\]
\[
(a + I) \times (b + I) = ab + I
\]

This is a source to many new rings
Examples

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

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

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

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

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 \( \varphi \),

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

\[
= 10a
\]
Circle ring

Let $R = \mathbb{R}[x, y]/(x^2 + y^2 - 1)$: 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?).
The circle ring $R = \mathbb{R}[\cos t, \sin t]$ contains as a subring $S = \mathbb{R}[\cos t]$. $S$ is isomorphic to a polynomial ring over $\mathbb{R}$. As an $S$-module, $R$ is generated by two elements

$$R = S \cdot 1 + S \cdot \sin t$$

$R$ as a $\mathbb{R}$-vector space has basis

$$\{\sin nt, \cos nt, \quad n \in \mathbb{Z}\}$$
Exercise: Prove that

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

**Hint:** 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.
Integral domains

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 $ab = 0$
- $a \in R$ is **nilpotent** if there is $n \in \mathbb{N}$ such that $a^n = 0$
- $R$ is an **integral domain** if $0$ is the only zero divisor, in other words, if $a, b \in R$ are not zero, then $ab \neq 0$. 
Outline

1. Rings and Modules
2. Chain Conditions
3. Assignment #6
4. **Prime Ideals**
5. Assignment #7
6. Primary Decomposition
7. Intro Noetherian Rings
8. Assignment #8
9. Homework
10. Modules of Fractions
11. Assignment #9
12. Integral Extensions
13. Integral Morphisms
14. Assignment #10
15. TakeHome #1
Studying a commutative ring

prime ideals of $R$  morphisms $\varphi : R \to S$
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 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

\[
\begin{array}{ccc}
R & \xrightarrow{\phi} & S \\
\downarrow & & \downarrow \\
R/P & & S/Q
\end{array}
\]
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

$$R = \mathbb{C}[x, y]/(y^2 - x(x - 1)(x - 2)).$$
Multiplicative Sets

**Definition**

A subset $S$ of a commutative ring is **multiplicative** if $S \neq \emptyset$ and if $r, s \in S$ then $r \cdot s \in S$.

- If $P$ is a prime ideal of $R$, $S = R \setminus P$ is a multiplicative set.
- If $I$ is a proper ideal of $R$, then
  
  \[ S = \{1 + a : a \in I\} \]

  is a multiplicative set.
Formation of Prime Ideals

**Proposition**

Let $S$ be a multiplicative set and $P$ an ideal maximum with respect $S \cap P = \emptyset$. Then $P$ is a prime ideal.

**Proof.** Deny: let $a, b \notin P$, $ab \in P$.

Consider the ideals $P + Ra$ and $P + Rb$. They are both larger than $P$ and therefore meet $S$:

$$x + pa, y + qb \in S, \quad x, y \in P$$

Multiplying we get

$$(x + pa)(y + qb) = xy + xqb + yqb + pqab \in S \cap P,$$

a contradiction.
Corollary

Every proper ideal $I$ of a commutative ring is contained in a prime ideal.

Proof. Let $S = \{1\}$. Among all proper ideals $I \subseteq J$ pick one that is maximum with respect being disjoint relative to $S$ (use Zorn’s Lemma; no need if $R$ is Noetherian).
Primary Ideal

Definition
Let $R$ be a commutative ring. An ideal $Q$ of $R$ is primary if $Q \neq R$ and whenever $a \cdot b \in Q$ then $a \in Q$ or some power $b^n \in Q$.

Example: $Q = (x^2, y) \subset R = k[x, y]$, or $(p^n) \subset \mathbb{Z}$. This is a far-reaching generalization of the notion of primary ideals of $\mathbb{Z}$.
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 $j \geq n$. 


Proposition

If $I$ is a proper ideal of $R$,

$$\sqrt{I} = \bigcap P, \quad I \subseteq P \quad P \text{ prime ideal}.$$ 

Proof.

Deny it: Let $x \in \bigcap P \setminus \sqrt{I}$, that is for all $n$, $x^n \notin I$.

The set $\{x^n, n \in \mathbb{N}\}$ defines a multiplicative set $S$ disjoint from $I$.

By a previous proposition, there is a prime $P \supset I$ disjoint from $S$, a contradiction.
A **Boolean ring** is a ring $R$ such that $x^2 = x$ for all $x \in R$. For instance, an arbitrary direct product of copies of $\mathbb{Z}/(2)$. If $R$ is a Boolean ring:

1. **Prove that $R$ is commutative and that for every prime ideal $P$, $R/P$ is a field.**
2. **Prove that every finitely generated ideal $I$ of $R$ is principal** (*Hint: check that in a boolean ring, $a + b - ab$ is a multiple of both $a$ and $b$).*
3. **If $R$ is finite, show that $R$ is a finite direct product of copies of $\mathbb{Z}/(2)$.**
Idempotents

Proposition

Let $R$ be a commutative ring and $0 \neq e \in R$ satisfy $e = e^2$. Then there is a decomposition $R$ into the direct product of rings $R \cong Re \times R(1 - e)$.

Proof.

1. For any $x \in R$, $x = xe + x(1 - e)$, so $Re + R(1 - e) = R$. Furthermore if $a \in Re \cap R(1 - e)$, then $a$ is annihilated by $1 - e$ and $e$, respectively. This means that $R = Re \oplus R(1 - e)$ as modules.

2. Since $Re \cdot R(1 - e) = 0$, we can view $R = Re \oplus R(1 - e)$ as $R = Re \times R(1 - e)$. Note that $e$ is the identity in the ring $Re$, and $1 - e$ in $R(1 - e)$. 

Outline

1. Rings and Modules
2. Chain Conditions
3. Assignment #6
4. Prime Ideals
5. Assignment #7
6. **Primary Decomposition**
7. Intro Noetherian Rings
8. Assignment #8
9. Homework
10. Modules of Fractions
11. Assignment #9
12. Integral Extensions
13. Integral Morphisms
14. Assignment #10
15. TakeHome #1
Emmy Noether (1882-1935)

http://upload.wikimedia.org/wikipedia/commons/e/e5/Noether.jpg
Irreducible Ideal/Module

Definition

The ideal $I$ of the commutative ring $R$ is irreducible if

$$I = J \cap L \Rightarrow I = J \quad \text{or} \quad I = L.$$
Primary Decomposition

Theorem (Emmy Noether)

Every proper ideal $I$ of a Noetherian ring $R$ has a finite decomposition

$$I = Q_1 \cap Q_2 \cap \cdots \cap Q_n,$$

with $Q_i$ primary.

To prove her theorems, Emmy Noether often proved a special case and derive the more general assertion, or proved a more general assertion and specialize.
Irreducible decomposition

**Definition**

The ideal $I$ of the commutative ring $R$ is **irreducible** if

$$I = J \cap L \Rightarrow I = J \text{ or } I = L.$$  

**Theorem (Emmy Noether)**

*Every proper ideal $I$ of a Noetherian ring $R$ has a finite decomposition*

$$I = J_1 \cap J_2 \cap \cdots \cap J_n,$$

*with $J_i$ irreducible. Moreover, every irreducible ideal $J$ of $R$ is primary.*
Proof. Deny the existence of the decomposition of $I$ as a finite intersection of irreducible ideals. Among all such ideals, denote by (keep the notation) $I$ a maximum one. $I$ is not irreducible, so there is

$$I = J \cap L,$$

with $J$ and $L$ properly larger. But then each admits finite decompositions as intersection of irreducible ideals. Combining we get a contradiction.
Deny that proper irreducible ideals of Noetherian rings are primary. Let \( I \) be maximum such: There is \( a, b \in R, \ ab \in I, \ a \notin I \) and \( b^n \notin I \) for all \( n \in \mathbb{N} \).

Consider the chain

\[
\{ r \in R : br \in I \} = I : b \subseteq I : b^2 \subseteq \cdots \subseteq I : b^n \subseteq I : b^{n+1}
\]

that becomes stationary at \( I : b^n = I : b^{n+1} \).

Define \( J = I : b^n \) and \( L = (I, b^n) \). Both ideals are larger than \( I \). We claim that \( I = J \cap L \).

If \( x \in J \cap L, \ x = u + rb^n, \ u \in I \). Then \( b^n x = b^n u + rb^{2n} \in I \), so \( rb^n \in I \) and therefore \( x \in I \).
Irredundant Primary Decomposition

A refinement in the primary decomposition

\[ I = Q_1 \cap Q_2 \cap \cdots \cap Q_n \]

arises as follows. Suppose two of the \( Q_i \) have the same radical, say \( \sqrt{Q_1} = \sqrt{Q_2} = P \). Then it easy to check that \( Q_1 \cap Q_2 \) is also \( P \)-primary. So collecting the \( Q_i \) with the same radical:

**Theorem (Emmy Noether)**

*Every proper ideal \( I \) of a Noetherian ring \( R \) has a finite decomposition*

\[ I = Q_1 \cap Q_2 \cap \cdots \cap Q_n, \]

*with \( Q_i \) primary ideals of distinct radicals. This decomposition is called irredundant.*

It is known which \( Q_i \) are unique and which are not.
Outline

1. Rings and Modules
2. Chain Conditions
3. Assignment #6
4. Prime Ideals
5. Assignment #7
6. Primary Decomposition
7. Intro Noetherian Rings
8. Assignment #8
9. Homework
10. Modules of Fractions
11. Assignment #9
12. Integral Extensions
13. Integral Morphisms
14. Assignment #10
15. TakeHome #1
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
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.
If $R$ is a commutative ring, a \textit{finitely generated} $R$-algebra $S$ is a homomorphic image of a ring of polynomials, $S = R[x_1, \ldots, x_n]/L$. If $R$ is Noetherian, $S$ is Noetherian as well. This is useful in many constructions.

If $I$ is an $R$-ideal, the \textit{Rees algebra of $I$} is the subring of $R[t]$ generated by all $at$, $a \in I$. It it denoted by $S = R[It]$. In general, subrings of Noetherian rings may not be Noetherian but Rees algebras are:

\textbf{Exercise:} If $R$ is Noetherian, for every ideal $I$, $R[It]$ 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,

$$f_1(x) = a_1 x^{d_1} + \text{lower degree terms.}$$

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

$$f_i(x) = a_i x^{d_i} + \text{lower degree terms},$$

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

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

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

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

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

\[
\begin{align*}
f(x) &= \sum_{n \geq 0} a_n x^n, & g(x) &= \sum_{n \geq 0} b_n x^n \\
\end{align*}
\]

with addition component wise and multiplication the Cauchy operation

\[
f(x)g(x) = h(x) = \sum_{n \geq 0} c_n x^n = \sum_{n \geq 0} \left( \sum_{i+j=n} a_i b_{n-i} \right)
\]

**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:

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

**Claim:** \(l = (b_1, \ldots, b_m, aa_1, \ldots, aa_n)\)

If \(c \in l\),

\[
c = \sum_{i=1}^{m} c_ib_i + ra, \quad r \in l : a
\]
$R[[x]]$ is Noetherian

**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

$$f(x) - \sum_i s_i^{(0)} f_i = x h \implies h \in P.$$
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

$$f(x) = \sum_{i} (s_i^{(0)} + s_i^{(1)} x + s_i^{(2)} x^2 + \cdots) f_i.$$
Outline

1. Rings and Modules
2. Chain Conditions
3. Assignment #6
4. Prime Ideals
5. Assignment #7
6. Primary Decomposition
7. Intro Noetherian Rings
8. **Assignment #8**
9. Homework
10. Modules of Fractions
11. Assignment #9
12. Integral Extensions
13. Integral Morphisms
14. Assignment #10
15. TakeHome #1
Assignment #8

Do 2 problems.

1. Show that the kernel of the homomorphism \( (K \text{ is a field}) \)
\[ \varphi : K[x, y, z] \rightarrow K[t], \]
defined by \( \varphi(x) = t^3, \varphi(y) = t^4 \) and \( \varphi(z) = t^5 \), is generated by the polynomials
\[ x^3 - yz, y^2 - xz, z^2 - x^2y. \]

2. Let \( R \) be a Noetherian ring and let \( I \) be an \( R \)-ideal. Show that the number of prime ideals \( P \) minimal over \( I \) is finite. 
(\text{Hint: primary decomposition helps.})

3. Describe all rings \( \mathbb{Z} \subset R \subset \mathbb{Q} \) (\text{Hint: For each } R, \text{ consider the set of primes } \rho \text{ of } \mathbb{Z} \text{ that blowup in } R, \text{ that is, } \rho R = R). \)

4. Let \( \varphi : M \rightarrow M \) be an endomorphism of a \( R \)-module. 
Prove that if \( M \) is Noetherian (resp. Artinian) and \( \varphi \) is surjective (resp. injective) then \( \varphi \) is an isomorphism.
Outline

1. Rings and Modules
2. Chain Conditions
3. Assignment #6
4. Prime Ideals
5. Assignment #7
6. Primary Decomposition
7. Intro Noetherian Rings
8. Assignment #8
9. Homework
10. Modules of Fractions
11. Assignment #9
12. Integral Extensions
13. Integral Morphisms
14. Assignment #10
15. TakeHome #1
Homework

1. Find the kernel of the homomorphism (K is a field)

\[ \varphi : K[x, y, z] \longrightarrow K[t], \]

defined by \( \varphi(x) = t^4, \varphi(y) = t^5 \) and \( \varphi(z) = t^7 \). What do you think is true in general?

2. Show that \( R = \mathbb{C}[x, y]/(y^2 - x(x - 1)(x - 2)) \) is a Dedekind domain. [Show that \( y^2 - x(x - 1)(x - 2) \) is irreducible, use the Nullstellensatz to describe the maximal ideals of \( R \), and show that for each such ideal \( P \), \( R_P \) is a discrete valuation domain.]

3. If \( R \) is a Dedekind domain, prove that for each nonzero ideal \( I \), \( R/I \) is a principal ideal ring. Derive from this the fact that every ideal of \( R \) can be generated by 2 elements.

4. Show that an invertible ideal of a local integral domain is principal.
Modules of Fractions

Let $R$ be a commutative ring, $M$ an $R$-module and $S \subseteq R$ a multiplicative system.

On the set $M \times S$ define the following relation:

$$(a, r) \sim (b, s) \iff \exists t \in S : t(as - br) = 0$$

Why define it in this manner instead of the usual $as = br$?

**Proposition**

$\sim$ is an equivalence relation.

We focus on the properties of the set $S^{-1}M$ of equivalence classes. Actually, this is the initial step in the construction of a remarkable functor.
Properties

Proposition

Let $R$ be a commutative ring, $M$ an $R$-module and $S \subseteq R$ a multiplicative system. Denote the equivalence class of $(a, r)$ in $S^{-1}M$ by $\overline{(a, r)}$ (or simply $(a, r)$ or even $a/r$).

1. The following operation is well-defined

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

and endows $S^{-1}M$ with a structure of abelian group.

2. If $0 \notin S$, this construction applied to $R \times S$ gives rise to a ring structure on $S^{-1}R$ with multiplication

$$(x, r) \cdot (y, s) = (xy, rs).$$

3. For $(x, r) \in S^{-1}R$ and $(a, s) \in S^{-1}M$, the operation

$$(x, r) \cdot (a, s) = (xa, rs)$$

defines an $S^{-1}R$-module structure on $S^{-1}M$. 

Module/Ring of Fractions

$S^{-1}R$ is called the ring of fractions of $R$ relative to $S$. It is a refinement (due to Grell or Krull) of the classical formation of the field of fractions of an integral domain. $S^{-1}M$ is called the module of fractions of $M$ relative to $S$.

Another step:

**Proposition**

If $\varphi : M \rightarrow N$ is a homomorphism of $R$-modules, a homomorphism of $S^{-1}R$ modules $S^{-1}\varphi : S^{-1}M \rightarrow S^{-1}N$ is defined by

$$(S^{-1}\varphi)(a, s) = (\varphi(a), s).$$
Functorial Properties

This construction is a functor from the category of $R$-modules to the category of $S^{-1}R$-modules:

$$
\begin{array}{ccc}
M & \sim & S^{-1}M \\
\varphi \downarrow & & \downarrow S^{-1}\varphi \\
N & \sim & S^{-1}N
\end{array}
$$

Proposition

If $\varphi : M \to N$ and $\psi : N \to P$ are $R$-homomorphisms of $R$-modules, then

1. $S^{-1}(\psi \circ \varphi) = S^{-1}\psi \circ S^{-1}\varphi.$
2. $S^{-1}(id_M) = id_{S^{-1}M}.$
Short Exact Sequences

Proposition

Let $R$ be a ring, $S \subseteq R$ a multiplicative set and

$$0 \rightarrow A \xrightarrow{f} B \xrightarrow{g} C \rightarrow 0$$

a short exact sequence of $R$-modules. Then

$$0 \rightarrow S^{-1} A \xrightarrow{S^{-1}f} S^{-1} B \xrightarrow{S^{-1}g} S^{-1} C \rightarrow 0$$

is a short exact sequence of $S^{-1} R$-modules. In other words, $M \mapsto S^{-1} M$ is an exact functor.
The submodules of $S^{-1}M$

**Proposition**

Let $L'$ be a $S^{-1}R$-submodule of $S^{-1}M$. Let

$$L = \{ m \in M : \text{for some } s \in S \ (m, s) \in L' \}. $$

Then $L$ is a submodule of $M$ and $S^{-1}L = L'$.

**Corollary**

If $M$ is a Noetherian (Artinian) $R$-module, then $S^{-1}M$ is a Noetherian (Artinian) $S^{-1}R$-module.
The ideals of $S^{-1}R$

According to the above, the proper ideals of $S^{-1}R$ are of the form

\[ S^{-1}I = \{a/s : a \in I, s \in S, \quad I \cap S = \emptyset\}. \]

In the special case of $S = R \setminus p$, for a prime ideal $p$, one uses the notation $M_p$ for the module of fractions and $R_p$ for the ring of fractions.

If $R = \mathbb{Z}$ and $p = (2)$, $\mathbb{Z}(2)$ consists of all rational numbers $m/n$, with $n$ odd. Its ideals are ordered. The largest proper ideal is $m = 2\mathbb{Z}(2)$ and the others

\[ \mathbb{Z}(2) \supset m \supset m^2 \supset m^3 \supset \cdots \supset (0) \]
Proposition

If $R$ is a commutative ring and $S$ is a multiplicative set, then for any two submodules $A$ and $B$ of $M$,

$$S^{-1}(A \cap B) = S^{-1}A \cap S^{-1}B.$$ 

Proof.

The intersection $A \cap B$ can be defined by the exact sequence

$$0 \to A \cap B \to A \oplus B \xrightarrow{\varphi} A + B \to 0,$$

where $\varphi(a, b) = a - b$.

Now apply the fact that formation of modules of fractions is an exact functor.
Local Ring

**Proposition**

Let $S$ be a multiplicative set of $R$. The ideal $L$ of $S^{-1}R$ is prime iff $L = S^{-1}I$, for some prime $I$ ideal of $R$ with $I \cap S = \emptyset$.

**Proof.** Suppose $I$ is as above. If $a/r \cdot b/s \in S^{-1}I$, $(ab, rs) \sim (c, t)$ for $c \in I$, $r, s, t \in S$. By definition, there is $u \in S$ such that $u(tab - rsc) = 0$. Since $S \cap I = \emptyset$, $tab - rsc \in I$ and therefore $tab \in I$. Thus $ab \in I$ and so $a \in I$ or $b \in I$. Therefore $(a, r)$ or $(b, s) \in S^{-1}I$.

**Corollary**

The prime ideals of $R_p$ have the form $P = Q_p$, where $Q$ is an ideal of $R$ contained in $p$. 
Local Ring

**Definition**

A commutative ring $R$ is a local ring if it has a unique maximal ideal.

**Example**

If $k$ is a field, $R = k[[x]]$, the ring of formal power series in $x$ over $k$ is a local ring. Its unique maximal ideal is $m = (x)$.

**Definition**

If $R$ is a commutative ring and $P$ a prime ideal, the ring of fractions $R_P$ is a local ring called the localization of $R$ at $P$. 
The Prime Spectrum of a Ring

Definition

Let $R$ be a commutative ring (with 1). The set of prime ideals of $R$ is called the prime spectrum of $R$, and denoted $\text{Spec}(R)$.

$\text{Spec}(\mathbb{Z}) = \{(0), (2), (3), \ldots\}$, the ideals generated by the prime integers and 0.

Proposition

For each set $I \subset R$, set

$$V(I) = \{p \in \text{Spec}(R) : I \subset p\}.$$  

These subsets are the closed sets of a topology on $\text{Spec}(R)$.

Note that $V(I) = V(I')$, where $I'$ is the ideal of $R$ generated by $I$. 
Zariski Topology

Proof. This follows from the properties of the construction of the $V(I)$:

$$
\begin{align*}
V(1) &= \emptyset \\
V(0) &= \text{Spec } (R) \\
V(I \cap J) &= V(I) \cup V(J) \\
\bigcap_{\alpha} V(I_{\alpha}) &= V(\bigcup_{\alpha} I_{\alpha}).
\end{align*}
$$
Example

Suppose $R_2, R_2, \ldots, R_n$ are commutative rings and $R = R_1 \times R_2 \times \cdots \times R_n$ is their direct product. Observe:

1. If $1 = e_1 + e_2 + \cdots + e_n$, $e_i \in R_i$, then $R_i = Re_i$ and $e_i e_j = 0$ if $i \neq j$.

2. Because of $e_i e_j = 0$ for $i \neq j$, if $P$ is a prime ideal of $R$ and some $e_i \notin P$ then the other $e_j \in P$. This shows $P = R_1 \times \cdots \times P_i \times \cdots \times R_n$, where $P_i$ is a prime ideal of $R_i$, $R/P = R_i/P_i$.

3. $	ext{Spec}(R) = \text{Spec}(R_1) \cup \cdots \cup \text{Spec}(R_n)$.

4. In particular, if $R_1 = R_2 = \cdots = R_n = \mathbf{K}$, $\mathbf{K}$ a field, the $	ext{Spec}(R)$ is a set of $n$ points with the discrete topology.
Irreducible Representation

**Proposition**

Let $I$ be an ideal of the Noetherian ring $R$ and let

$$I = Q_1 \cap Q_2 \cap \cdots \cap Q_n,$$

be a primary representation. Then

$$V(I) = V(P'_1) \cup V(P'_2) \cup \cdots \cup V(P'_m),$$

where the $P'_j$ are the minimal primes amongst the $\sqrt{Q_i}$, is the unique irreducible representation of $V(I)$.
**Morphisms**

**Proposition**

If $R$ is a commutative ring, $\text{Spec}(R)$ is quasi-compact. (Not necessarily Hausdorff.)

**Proof.**

Let $\{D(I_\alpha)\}$ be an open cover of $X$

$$X = \bigcup_{\alpha} D(I_\alpha) = \sum_{\alpha} I_\alpha = D(1).$$

This means that there is a finite sum

$$\sum_{i=1}^{n} I_{\alpha_i} = R,$$

and therefore $X = \bigcup_{i=1}^{n} D(I_{\alpha_i}).$
Proposition

If \( \varphi : R \rightarrow S \) is a homomorphism of commutative rings \((\varphi(1_R) = 1_S)\), then the mapping

\[
\Phi : \text{Spec} (S) \rightarrow \text{Spec} (R),
\]

given by \( \Phi(Q) = \varphi^{-1}(Q) \), is continuous.

Proof.

If \( D(I) \) is an open set of \( \text{Spec} (R) \), \( \varphi^{-1}(D(I)) = D(IS) \).
Assignment #9

Do 1 problem.
For the ring $R = \mathbb{Z}[T]$

1. Describe (with proofs) its prime ideals, that is the points of $\text{Spec} \ (R)$.

2. Describe (with proofs) its maximal ideals, that is the closed points of $\text{Spec} \ (R)$.

3. Let $X$ be a compact, Hausdorff space and denote by $A$ the ring of real continuous functions on $X$.
   - If $M$ is a maximal ideal of $A$ prove that there is a point $p \in X$ such that $M = \{ f(x) \in A : f(p) = 0 \}$.
   - Prove that there is a homeomorphism of topological spaces $X \approx \text{MaxSpec}(A)$. 
Outline

1. Rings and Modules
2. Chain Conditions
3. Assignment #6
4. Prime Ideals
5. Assignment #7
6. Primary Decomposition
7. Intro Noetherian Rings
8. Assignment #8
9. Homework
10. Modules of Fractions
11. Assignment #9
12. **Integral Extensions**
13. Integral Morphisms
14. Assignment #10
15. TakeHome #1
Integral Extensions

Let $R \hookrightarrow S$ be commutative rings.

**Definition**

$s \in S$ is integral over $R$ if there is an equation

$$s^n + a_{n-1}s^{n-1} + \cdots + a_1 s + a_0 = 0, \quad a_i \in R.$$ 

**Proposition**

$s \in S$ is integral over $R$ if and only if the subring $R[s]$ of $S$ generated by $s$ is a finitely generated $R$-module.
Would like to prove [as done first by Weierstrass] that if \( s_1 \) and \( s_2 \) in \( S \) are integral over \( R \) then

- \( s_1 + s_2 \) is integral over \( R \);
- \( s_1 s_2 \) is integral over \( R \).

The key to their proof is the fact that both \( s_1 + s_2 \) and \( s_1 s_2 \) are elements of the subring \( R[s_1, s_2] \) which is finitely generated as an \( R \)-module

\[
R[s_1, s_2] = \sum_{i,j} R s_1^i s_2^j,
\]

where \( i \) and \( j \) are bounded by the degrees of the equations satisfied by \( s_1 \) and \( s_2 \).
Integrality Criterion

**Proposition**

Let $M$ be a finitely generated $R$-module and $S = R[u]$ a ring such that $uM \subset M$. If $M$ is a faithful $S$-module then $u$ is integral over $R$.

**Proof.** Let $x_1, \ldots, x_n$ be a set of $R$-generators of $M$. we have a set of relations with $a_{ij} \in R$

\[
ux_1 = a_{11}x_1 + \cdots + a_{1n}x_n \\
\vdots \\
u x_n = a_{n1}x_1 + \cdots + a_{nn}x_n
\]
Cayley-Hamilton

That is

\[ 0 = (a_{11} - u)x_1 + \cdots + a_{1n}x_n \]
\[ \vdots \]
\[ 0 = a_{n1}x_1 + \cdots + (a_{nn} - u)x_n \]

Which we rewrite in matrix form

\[
\begin{bmatrix}
  a_{11} - u & \cdots & a_{1n} \\
  \vdots & \ddots & \vdots \\
  a_{n1} & \cdots & a_{nn} - u
\end{bmatrix}
\begin{bmatrix}
  x_1 \\
  \vdots \\
  x_n
\end{bmatrix}
= \begin{bmatrix}
  0 \\
  \vdots \\
  0
\end{bmatrix}
= A[x] = O.
\]
Thus

\[(\text{adj } A)A[x] = \det A \cdot [x] = O.\]

This means that \(\det A\) annihilates each generator \(x_i\) of \(M\) and therefore \(\det A = 0\).

But

\[\det A = \pm u^n + \text{lower powers of } u \text{ with coefficients in } R\]

This shows that \(u\) is integral over \(R\).
Why are we allowed to write $\text{adj } \mathbf{A} \cdot \mathbf{A} = \det \mathbf{A} \cdot \mathbf{I}$ when the entries of $\mathbf{A}$ lie in a commutative ring?

If $T = \mathbb{Z}[x_{ij}, 1 \leq i, j \leq n]$ is a ring of polynomials in the indeterminates $x_{ij}$, and use them as the entries of a matrix $\mathbf{B}$, certainly the formula $\text{adj } \mathbf{B} \cdot \mathbf{B} = \det \mathbf{B} \cdot \mathbf{I}$ makes sense since $T$ lies in a field.

Now define a ring homomorphism $\phi : T \to R$, with $\phi(x_{ij})$ the corresponding entry in $\mathbf{A}$, to get the desired equality.
In our application, $M = R[s_1, s_2]$ and $u$ is either $s_1 + s_2$ or $s_1 s_2$, and certainly $M$ is faithful since $1 \in M$.

**Corollary**

If $R \hookrightarrow S$ are commutative rings, and $s_1, s_2, \ldots, s_n$ are integral over $R$, then any element of $R[s_1, \ldots, s_n]$ is integral over $R$. Moreover, if $T$ is the set of elements of $S$ integral over $R$, $T$ is a subring. It is called the integral closure of $R$ in $S$.

**Definition**

If $T = S$, $S$ is called an integral extension of $R$. 
Transitivity

**Proposition**

If $R \hookrightarrow S_1 \hookrightarrow S_2$ are commutative rings with $S_1$ integral over $R$ and $S_2$ integral over $S_1$, then $S_2$ is integral over $R$.

**Proof.** Let $u \in S_2$ be integral over $S_1$

$$u^n + s_{n-1}u^{n-1} + \cdots + s_1u + s_0 = 0, \quad s_i \in S_1.$$  

It suffices to observe that

$$M = R[u, s_{n-1}, \ldots, s_1, s_0]$$

is a finitely generated $R$-module.
Surjections

Another use of the Cayley-Hamilton theorem is the following property of surjective epimorphims of modules:

**Theorem**

Let $R$ be a commutative ring and $M$ a finitely generated $R$. If $\varphi : M \to M$ is a surjective $R$-module homomorphism, then $\varphi$ is an isomorphism.

**Proof.** We first turn $M$ into a module over the ring of polynomials $S = R[t]$ by setting $t \cdot m = \varphi(m)$ for $m \in M$.

The assumption means that $tM = M$. Using the proof of Cayley-Hamilton, we have
\[
\begin{bmatrix}
ta_{11} - 1 & \cdots & ta_{1n} \\
\vdots & \ddots & \vdots \\
ta_{n1} & \cdots & ta_{nn} - 1
\end{bmatrix}
\begin{bmatrix}
x_1 \\
\vdots \\
x_n
\end{bmatrix}
= \begin{bmatrix}
0 \\
\vdots \\
0
\end{bmatrix}
= A[x] = O.
\]

Which implies that \( \det A \) annihilates \( M \). Since

\[\det A = \pm 1 + tf(t),\]

it is clear that \( t \cdot m \neq 0 \) for \( m \neq 0 \), that is \( \phi \) is one-to-one.
Jacobson Radical

Definition
Let $R$ be a commutative ring. Its Jacobson radical is the intersection $\bigcap Q$ of all maximal (proper) ideals.

Example: If $R$ is a local ring, its Jacobson radical is its unique maximal ideal $m$.

If $R = \mathbb{Z}$, or $R = k[t]$, polynomial ring over the field $k$, then $(0)$ is the Jacobson radical: from the infinity of prime elements.
Proposition

The Jacobson radical $J$ of $R$ is the set

$$J' = \{ a \in R : 1 + ra \text{ is invertible for all } r \in R \}.$$

Proof. If $a \in J$, then $1 + ra$ cannot be contained in any proper maximal ideal, that is it must be invertible.
Conversely, if $a \in J'$, suppose $a$ does not belong to the maximal ideal $Q$. Therefore

$$(a, Q) = R$$

which means there is an equation $ra + q = 1$, $q \in Q$, and $q$ would be invertible.
Nakayama Lemma

**Theorem (Nakayama Lemma)**

Let $M$ be a finitely generated $R$ module and $J$ its Jacobson radical. If

$$M = JM,$$

then $M = 0$.

**Proof.** If $M$ is cyclic, this is clear: $M = (x)$ implies $x = ux$ for some $u \in J$, so that $(1 - u)x = 0$, which implies $x = 0$ since $1 - u$ is invertible.

We are going to argue by induction on the minimal number of generators of $M$. Suppose $M = (x_1, \ldots, x_n)$. By assumption $x_1 \in JM$, that is we can write

$$x_1 = u_1 x_1 + u_2 x_2 + \cdots + u_n x_n, \quad u_i \in J.$$
Which we rewrite as

\[(1 - u_1)x_1 = u_2x_2 + \cdots + u_nx_n\]

This shows that \(x_1 \in J(x_2, \ldots, x_n)\), and therefore \(M = (x_2, \ldots, x_n)\).

**Corollary**

Let \(M\) be a finitely generated \(R\) module and \(N\) a submodule. If \(M = N + JM\) then \(M = N\).

**Proof.**

Apply the Nakayama Lemma to the quotient module \(M/N\)

\[M/N = N + JM/N = J(M/N).\]
Scholium

Let $R$ be a commutative ring and $M$ a finitely generated $R$-module. If for some ideal $I$, $IM = M$, then $(1 + a)M = 0$ for some $a \in I$.

Proof.

If $M = (x_1, \ldots, x_n)$, from the proof of Cayley-Hamilton, there are $a_{ij} \in I$

$$
\begin{bmatrix}
    a_{11} - 1 & \cdots & a_{1n} \\
    \vdots & \ddots & \vdots \\
    a_{n1} & \cdots & a_{nn} - 1
\end{bmatrix}
\begin{bmatrix}
    x_1 \\
    \vdots \\
    x_n
\end{bmatrix}
= \begin{bmatrix}
    0 \\
    \vdots \\
    0
\end{bmatrix} = A[x] = 0.
$$

Which implies that $\det A$ annihilates $M$. Since $\det A = \pm 1 + a$, $a \in I$, done.
Corollary

Let $R$ be a commutative ring and $I$ a finitely generated ideal. Then $I = I^2$ if and only if $I$ is generated by an idempotent, that is $I = Re, e^2 = e$.

Proof.

If $(1 + a)I = 0$, $I \subset (a)$ and $a^2 = a$. 

$\square$
Outline

1. Rings and Modules
2. Chain Conditions
3. Assignment #6
4. Prime Ideals
5. Assignment #7
6. Primary Decomposition
7. Intro Noetherian Rings
8. Assignment #8
9. Homework
10. Modules of Fractions
11. Assignment #9
12. Integral Extensions
13. Integral Morphisms
14. Assignment #10
15. TakeHome #1
Integral Morphisms

Let \( \varphi : R \to S \) an injective homomorphism of commutative rings.

**Theorem (Lying-Over Theorem)**

If \( S \) is integral over \( R \) then for each \( \mathfrak{p} \in \text{Spec}(R) \) there is \( P \in \text{Spec}(S) \) such that \( \mathfrak{p} = P \cap R \), that is the morphism

\[
\text{Spec}(S) \to \text{Spec}(R)
\]

is surjective.
Proposition

If $S$ is integral over $R$ and $T$ is a multiplicative set of $R$, then $T^{-1}S$ is integral over $T^{-1}R$.

Proof.

Let $s/t \in T^{-1}S$. $s$ satisfies an equation

$$s^n + a_{n-1}s^{n-1} + \cdots + a_1s + a_0 = 0, \quad a_i \in R.$$ 

Then

$$(s/t)^n + a_{n-1}/t(s/t)^{n-1} + \cdots + a_1/t^{n-1}s/t + a_0/t^n = 0,$$

$$a_i/t^{n-i} \in T^{-1}R.$$
Proof of Lying-Over

Suppose \( p \in \text{Spec}(R) \). Consider the integral extension \( R_p \hookrightarrow S_p \).

The maximal ideal of \( R_p \) is \( m = pR_p \).

**Claim:** \( mS_p \neq S_p \).

Otherwise we would have

\[
1 \in mS_p
\]

\[
1 = \sum_{i=1}^{n} a_is_i/t_i, \quad a_i \in m, \quad s_i \in S, \quad t_i \in R \setminus p
\]
1. Set $S' = R_p[s_1, \ldots, s_n]$.
2. $S'$ is a finitely generated $R_p$-module with $S' = mS'$. By Nakayama Lemma, $S' = 0$.
3. Since $mS_p \neq S_p$, it is contained in a prime ideal $P'$ of $S_p$. In particular, $P' \cap R_p = m$.
4. Since $P' = p_P$ for some $P \in \text{Spec}(S)$, it is clear that $P \cap R = p$, as desired.
Going-Up Theorem

**Theorem**

Let \( R \hookrightarrow S \) be an integral extension of commutative rings. Let \( p_1 \subsetneq p_2 \) be prime ideals of \( R \) and suppose \( P_1 \) is a prime ideal of \( S \) such that \( P_1 \cap R = p_1 \). Then there is a prime ideal \( P_1 \subsetneq P_2 \) of \( S \) such that \( P_2 \cap R = p_2 \).

**Proof.** Consider the diagram

\[
\begin{array}{ccc}
R & \hookrightarrow & S \\
\downarrow & & \downarrow \\
R/p_1 & \hookrightarrow & S/P_1
\end{array}
\]

Now apply the Lying-Over theorem to the integral extension

\( R/p_1 \hookrightarrow S/P_1 \).
Going-Down Theorem

? Is there

**Theorem (Going-Down Theorem)**

Let $R \hookrightarrow S$ be an integral extension of commutative rings. Let $p_1 \subsetneq p_2$ be prime ideals of $R$ and suppose $P_2$ is a prime ideal of $S$ such that $P_2 \cap R = p_2$. Then there is a prime ideal $P_1 \subsetneq P_2$ of $S$ such that $P_1 \cap R = p_1$.

Yes, but needs additional assumptions. Proof uses some basic Galois theory.
Let $R \hookrightarrow S$ be an integral extension. Prove the following assertions:

1. If $R$ and $S$ are integral domains and one of them is a field, then the other is also a field.

2. Equivalently: Let $P \in \text{Spec}(S)$ and $p \in \text{Spec}(R)$ and $P \cap R = p$. Then $P$ is maximal iff $p$ is maximal.
Outline

1. Rings and Modules
2. Chain Conditions
3. Assignment #6
4. Prime Ideals
5. Assignment #7
6. Primary Decomposition
7. Intro Noetherian Rings
8. Assignment #8
9. Homework
10. Modules of Fractions
11. Assignment #9
12. Integral Extensions
13. Integral Morphisms
14. Assignment #10
15. TakeHome #1
Take Home #1

Do 5 problems.

- Describe [with proof] a method to construct a regular pentagon with ruler and compass.
- Show that if \( n \geq 3 \), then \( x^{2n} + x + 1 \) is reducible over \( \mathbb{Z}_2 \).
- Describe (with proofs) the maximal ideals of \( R = \mathbb{Z}[T] \), that is the closed points of \( \text{Spec} (R) \). \textbf{Achtung:} Pay attention to polynomials such as \( aT - 1 \).
- Let \( R = k[x_1, \ldots, x_n, \ldots] \), the ring of polynomials in a countable set of indeterminates over the field \( k \). Prove that every ideal of \( R \) admits a countable number of generators.
- Find the kernel of the homomorphism (\( K \) is a field)
  \[
  \varphi : K[x, y, z] \longrightarrow K[t],
  \]
  defined by \( \varphi(x) = t^4 \), \( \varphi(y) = t^5 \) and \( \varphi(z) = t^7 \).
- \( \varphi : \mathbb{Q}/\mathbb{Z} \rightarrow \mathbb{Q}/\mathbb{Z} \) is a one-one group homomorphism, prove it is onto. (You may want to look at the action on the primary components.)