Advanced Algebra II
Mar. 9, 2007
Proposition

1. If $I \triangleleft R$, then $S^{-1}I \triangleleft S^{-1}R$. Moreover, every ideal $J \triangleleft S^{-1}R$ is of the form $S^{-1}I$ for some $I \triangleleft R$. 
Proposition

1. If $I \triangleleft R$, then $S^{-1}I \triangleleft S^{-1}R$. Moreover, every ideal $J \triangleleft S^{-1}R$ is of the form $S^{-1}I$ for some $I \triangleleft R$.

2. For $J \triangleleft S^{-1}R$, then $S^{-1}(J \cap R) = J$. 

Proposition

1. If $I \triangleleft R$, then $S^{-1}I \triangleleft S^{-1}R$. Moreover, every ideal $J \triangleleft S^{-1}R$ is of the form $S^{-1}I$ for some $I \triangleleft R$.
2. For $J \triangleleft S^{-1}R$, then $S^{-1}(J \cap R) = J$.
3. $S^{-1}I = S^{-1}R$ if and only if $I \cap S \neq \emptyset$. 
Proposition

1. If $I \triangleleft R$, then $S^{-1}I \triangleleft S^{-1}R$. Moreover, every ideal $J \triangleleft S^{-1}R$ is of the form $S^{-1}I$ for some $I \triangleleft R$.

2. For $J \triangleleft S^{-1}R$, then $S^{-1}(J \cap R) = J$.

3. $S^{-1}I = S^{-1}R$ if and only if $I \cap S \neq \emptyset$.

4. There is a one-to-one correspondence between 
   \[ \{ p \in \text{Spec}(R) | p \cap S = \emptyset \} \text{ and } \{ q \in \text{Spec}(S^{-1}R) \}. \]
Proposition

1. If $I \triangleleft R$, then $S^{-1}I \triangleleft S^{-1}R$. Moreover, every ideal $J \triangleleft S^{-1}R$ is of the form $S^{-1}I$ for some $I \triangleleft R$.

2. For $J \triangleleft S^{-1}R$, then $S^{-1}(J \cap R) = J$.

3. $S^{-1}I = S^{-1}R$ if and only if $I \cap S \neq \emptyset$.

4. There is a one-to-one correspondence between\n\{$p \in \text{Spec}(R) | p \cap S = \emptyset$\} and \{$q \in \text{Spec}(S^{-1}R)$\}.

5. In particular, the prime ideals of the local ring $R_p$ are in one-to-one correspondence with the prime ideals of $R$ contained in $p$. 
But for $I \triangleleft R$, then $S^{-1}I \cap R \supset I$ only.
Indeed, if $x \in I \triangleleft R$. Then $x = \frac{xs}{x} \in S^{-1}I \cap R$.
Conversely, for $x \in S^{-1}I \cap R$, then $\frac{x}{I} = \frac{y}{t}$ for some $y \in I$.
Thus $(y - xt)s = 0$ for some $s, t \in S$. We can not get $y \in I$ in general.
However, this is the case if $I$ is prime and $S \cap I = \emptyset$. Thus we have
But for $I \triangleleft R$, then $S^{-1}I \cap R \supset I$ only.

Indeed, if $x \in I \triangleleft R$. Then $x = \frac{xs}{x} \in S^{-1}I \cap R$.

Conversely, for $x \in S^{-1}I \cap R$, then $\frac{x}{I} = \frac{y}{t}$ for some $y \in I$.

Thus $(y - xt)s = 0$ for some $s, t \in S$. We can not get $y \in I$ in general.

However, this is the case if $I$ is prime and $S \cap I = \emptyset$. Thus we have

**Proposition**

*If $p \triangleleft R$ is a prime ideal and $S \cap p = \emptyset$. Then $S^{-1}p \cap R = p$.***
Example

Let $p \in \text{Spec}(R)$, then $R_p$ is a local ring with the unique maximal ideal $pR_p$. 
Example

Let \( p \in \text{Spec}(R) \), then \( R_p \) is a local ring with the unique maximal ideal \( pR_p \).

To see this, if there is a maximal ideal \( m \). By the correspondence, \( m = qR_p \) for some \( q \subset p \). Thus \( m \subset pR_p \) and thus must be equal. A ring with a unique maximal ideal is called a local ring. Thus \( R_p \) is a local ring.
Example

More explicitly, we can consider the following example. Let $R = k[x, y, x]$ and $p = (x, y)$. Then there is a chain of prime ideals:

0 $\subset$ $(x)$ $\subset$ $(x, y)$ $\subset$ $(x, y, z)$ $\subset$ $R$.

If we look at $R/p \cong k[z]$, we see a chain of prime ideals 0 $\subset$ $(z)$ $\subset$ $k[z]$, which corresponds to $(x, y)$ $\subset$ $(x, y, z)$ $\subset$ $R$ in $(\ast)$.

This has the following geometric interpretation: by looking at the ring $R/p$, we understand the "polynomial functions" on the set defined by $x = 0$, $y = 0$, i.e. the $z$-axis. On the other hand, if we look at $R/p$, we see a chain of prime ideals 0 $\subset$ $(x)$ $\subset$ $(x, y)$ $\subset$ $(x, y, z)$ $\subset$ $R$ in $(\ast)$.

Geometrically, it can be think as "local functions near a "generic" point in $z$-axis." We will come to more precise description of "polynomial functions" and generic point later.
Example

More explicitly, we can consider the following example. Let \( R = k[x, y, z] \) and \( \mathfrak{p} = (x, y) \). Then there is a chain of prime ideals:

\[
0 \subset (x) \subset (x, y) \subset (x, y, z) \subset R.
\]  

(\*)

If we look at \( R/\mathfrak{p} \cong k[z] \), we see a chain of prime ideals

\[
0 \subset (z) \subset k[z],
\]

which corresponds to \( (x, y) \subset (x, y, z) \subset R \) in (\*). This has the following geometric interpretation:

by looking at the ring \( R/\mathfrak{p} \), we understand the "polynomial functions" on the set defined by \( x = 0, y = 0 \), i.e. the \( z \)-axis.
Example

More explicitly, we can consider the following example. Let $R = k[x, y, z]$ and $p = (x, y)$. Then there is a chain of prime ideals:

$$0 \subset (x) \subset (x, y) \subset (x, y, z) \subset R.$$  

If we look at $R/p \cong k[z]$, we see a chain of primes ideals $0 \subset (z) \subset k[z]$, which corresponds to $(x, y) \subset (x, y, z) \subset R$ in $(*)$. This has the following geometric interpretation:

by looking at the ring $R/p$, we understand the ”polynomial functions” on the set defined by $x = 0, y = 0$, i.e. the $z$-axis.

On the other hand, if we look at $R_p$, we see a chain of primes ideals $0 \subset (x)R_p \subset (x, y)R_p$ which corresponds to $0 \subset (x) \subset (x, y)$ in $(*)$.

Geometrically, it can be think as ”local functions near a ”generic” point in $z$-axis.

We will come to more precise description of ”polynomial functions” and generic point later.
Proposition

The operation $S^{-1}$ on ideals commutes with formation of finite sums, product, intersection and radicals.
It’s essential to study modules in ring theory. One might find that modules not only generalize the notion of ideals but also clarify many things.

**Definition**

*Let R be a ring. An abelian group M is said to be an R-module if there is a map \( \mu : R \times M \rightarrow M \) such that for all \( a, b \in R \), \( x, y \in M \), we have:*

\[
\begin{align*}
  a(x + y) &= ax + ay \\
  (a + b)x &= ax + bx \\
  a(bx) &= (ab)x \\
  1x &= x
\end{align*}
\]
Example

Let $R$ be a ring and $I \triangleleft R$ be an ideal. Then $I$, $R/I$ are $R$-modules naturally.
Example

Let $R$ be a ring and $I \triangleleft R$ be an ideal. Then $I$, $R/I$ are $R$-modules naturally.

Example

An abelian group $G$ has a natural $\mathbb{Z}$-module structure by $\mu(m, g) := mg$ for all $m \in \mathbb{Z}$ and $g \in G$. 

Note that let $M, N$ be $R$-modules. By a $R$-module homomorphism, we mean a group homomorphism

$$\varphi : M \rightarrow N$$

such that $\varphi(rx) = r\varphi(x)$. That is, it’s an $R$-linear map.
Note that let $M, N$ be $R$-modules. By a $R$-module homomorphism, we mean a group homomorphism
\[ \varphi : M \to N \]
such that $\varphi(rx) = r\varphi(x)$.
That is, it’s an $R$-linear map.

**Exercise**

Given an $R$-module homomorphism
\[ f : M \to N, \]
then $\ker(f)$, $\text{im}(f)$, $\text{coker}(f)$ are $R$-modules in a natural way.
Let $M$ be an $R$-module. Given $x \in M$, then $Rx$ is a submodule of $M$. Even $Ix$ is a submodule for any ideal $I \triangleleft R$. More generally, $IN$ is a submodule of $M$ if $N < M$ and $I \triangleleft R$.

On the other hand, given $x \in M$, we may consider the annihilator of $x$, 

$$Ann(x) := \{ r \in R | rx = 0 \}.$$ 

It’s clear to be an ideal. Also for any submodule $N < M$. We can define $Ann(N)$ similarly as $\{ r \in R | rN = 0 \}$. 
A remark is that for a $R$-module $M$, the module structure map $R \times M \to M$ also induces a natural map $R/\text{Ann}(M) \times M \to M$. Hence $M$ can also be viewed as $R/\text{Ann}(M)$-module. Note that for given $x \in M$, the natural map $f : R \to Rx$ is a $R$-linear map. And $\ker(f) = \text{Ann}(x)$. So in fact, we have an $R$-module isomorphism $R/\ker(f) \cong Rx$ by the isomorphism theorem.

**Definition**

A element $x \in M$ is said to be torsion if $\text{Ann}(x) \neq 0$. A module is torsion if every non-zero element is torsion. A module is torsion-free if every non-zero element is not torsion.
Exercise

Given two modules $M, N$, note that the set of all $R$-module homomorphisms, denoted $\text{Hom}(M, N)$, is naturally an $R$-module.
Another important feature is that

**Proposition**

The operation $S^{-1}$ is exact. That is, if

$$
M' \xrightarrow{f} M \xrightarrow{g} M''
$$

is an exact sequence of $R$-module, then

$$
S^{-1}M' \xrightarrow{S^{-1}f} S^{-1}M \xrightarrow{S^{-1}g} S^{-1}M''
$$

is exact as $S^{-1}R$-module.
Corollary

The operation $S^{-1}$ commutes with passing to quotients by ideals. That is, let $I \triangleleft R$ be an ideal and $\tilde{S}$ the image of $S$ in $\tilde{R} := R/I$. Then $S^{-1}R/S^{-1}I \cong \tilde{S}^{-1}\tilde{R}$. 
We now introduce a very important and useful Lemma, Nakayama’s Lemma.

Theorem
Let $M$ be a finitely generated $R$-module. Let $a \subset J(R)$ be an ideal contained in the Jacobson radical. Then $aM = M$ implies $M = 0$.

Perhaps the most useful case is when $(R, m)$ is a local ring. Then $J(R) = m$ is nothing but the unique maximal ideal. The assertion is that if $mM = M$, then $M = 0$. 
We now introduce a very important and useful Lemma, Nakayama’s Lemma.

**Theorem**

*Let $M$ be a finitely generated $R$-module. Let $\mathfrak{a} \subseteq \mathfrak{J}(R)$ be an ideal contained in the Jacobson radical. Then $\mathfrak{a}M = M$ implies $M = 0$.***

Perhaps the most useful case is when $(R, m)$ is a local ring. Then $\mathfrak{J}(R) = m$ is nothing but the unique maximal ideal. The assertion is that if $mM = M$, then $M = 0$.***
We now introduce a very important and useful Lemma, Nakayama’s Lemma.

Theorem

Let $M$ be a finitely generated $R$-module. Let $\mathfrak{a} \subset \mathfrak{J}(R)$ be an ideal contained in the Jacobson radical. Then $\mathfrak{a}M = M$ implies $M = 0$.

Perhaps the most useful case is when $(R, \mathfrak{m})$ is a local ring. Then $\mathfrak{J}(R) = \mathfrak{m}$ is nothing but the unique maximal ideal. The assertion is that if $\mathfrak{m}M = M$, then $M = 0$. 
Proof.
Suppose $M \neq 0$.
Let $x_1, ..., x_n$ be a minimal generating set of $M$. We shall prove by induction on $n$.
Note that for an ideal $I \triangleleft R$, elements in $IM$ can be written as $a_1x_1 + ... + a_nx_n$ for $a_i \in I$.
Since $\alpha M = M$, we have $x_1 = \sum_{i=1}^{n} a_ix_i$ for $a_i \in \alpha$. Hence we have $(1 - a_1)x_1 = \sum_{i=2}^{n} a_ix_i$.
Notice that $(1 - a_1)$ is a unit, otherwise it’s in some maximal ideal which leads to a contradiction.
So we have either $x_1 = 0$ or $x_1$ is generated by $x_2, ..., x_n$. Either one is a contradiction. \qed
By applying the Lemma to \( M/N \), and note that 
\[ a(M/N) = (aM + N)/N, \] 
we have the following:

**Corollary**

Keep the notation as above, if \( N < M \) is a submodule such that 
\( M = aM + N \), then \( M = N \).

**Corollary**

Let \( R \) be a local ring and \( M \) be a finitely generated \( R \)-module. If 
\( x_1, \ldots, x_n \) generates \( M/mM \) as a vector space, then \( x_1, \ldots, x_n \) generates \( M \).
We close this section by considering finitely generated modules over PID. We have two important and interesting examples.
Example

Let $G$ be a finitely generated abelian group. Then it’s clearly a $\mathbb{Z}$-module while $\mathbb{Z}$ is PID.
Moreover, a finite group is clearly a torsion module.
Example

Let $V$ be a $n$-dimensional vector space over $k$. Let $A$ be a $n \times n$ matrix over $k$ (or a linear transform from $V$ to $V$). Then $V$ can be viewed as a $k[t]$-module via $k[t] \times V \to V$, with $f(t)v \mapsto f(A)v$. Note that by Cayley-Hamilton Theorem, $f(A) = 0$ for $f(x)$ being the characteristic polynomial. In fact, $Ann(V) = (p(x))$, where $p(x)$ is the minimal polynomial of $A$. Therefore, $V$ is a torsion module.
Now let $M$ be a finitely generated torsion module over a PID $R$. One sees that $\text{Ann}(M) \neq 0$. Since $R$ is PID, we have $\text{Ann}(M) = \prod (p_i^{a_i})$. For each $p_i$, we consider $M(p_i) := \{x \in M | p_i^n x = 0, \text{ for some } n\}$. One can prove that $M = \bigoplus M(p_i)$. In fact, for each $p_i$, there exist $n_1 \geq n_2 \geq ... \geq n_j$ such that $M(p_i) \cong \bigoplus_{k=1}^{j_i} R/(p_i^{n_k})$. These $p_i^{n_k}$ are called elementary divisors.
Apply this discussion to the example of linear transformation. Then $Ann(V) = (p(x))$. We assume that $p(x) = \prod (x - \lambda_i)^{a_i}$ splits into linear factors.

$V(\lambda_i) = \text{generalized eigenspace of } \lambda_i$.

$V = \bigoplus V(\lambda_i)$: the decomposition into generalized eigenspaces.

$V(\lambda_i) \cong \bigoplus_{k=1}^{j_i} k[x]/((x - \lambda_i)^{n_k})$: further decomposition of eigenspaces into invariant subspaces. The restriction of linear transformation into these invariant subspaces gives a Jordan block.
More explicitly, suppose that we have \( \nu \in V \) which corresponds to a generator of \( k[t]/(x - \lambda_i)^m \). Then we have independent vectors:

\[
\nu = \nu_0, (A - \lambda_i)\nu = \nu_1, \ldots, (A - \lambda_i)^{m-1}\nu = \nu_{m-1}.
\]

Using this set as part of basis, then we see

\[
A\nu_0 = \lambda_i \nu_0 + \nu_1, \\
\vdots \\
A\nu_{m-2} = \lambda_i \nu_{m-2} + \nu_{m-1}, \\
A\nu_{m-1} = \lambda_i \nu_{m-1}
\]

This gives the Jordan block