Advanced Algebra II
Apr. 13, 2007
Before we go to dimension theory, we would like to investigate integral extension a little bit more which will be useful in Dedekind domain and DVRs. Integral extension is very similar to algebraic extension.

**Definition**

A domain $A$ is said to be integrally closed if it is integrally closed in its quotient field.

For the rest of this section, we are going to assume that $B$ is a domain integral over $A$ and $A$ is integrally closed (i.e., in its quotient field $K$). We remark that this setting is closely related to algebraic field extensions.
Lemma

Let \( A \subset B \) be an extension and \( C \) is the integral closure of \( A \) in \( B \). Let \( a \triangleleft A \) be an ideal. We say that \( b \in B \) is integral over \( a \) if \( b \) satisfies a polynomial with coefficient (except the leading term) in \( a \). Then the integral closure of \( a \) in \( B \) is \( \sqrt{aC} \).
Proof.
If \( b \in B \) is integral over \( a \), then

\[ b^n + a_{n-1}b^{n-1} + ... + a_0 = 0. \]

Since \( b \in C \), we have

\[ b^n = -a_{n-1}b^{n-1} - ... - a_0 \in aC. \]

Thus \( b \in \sqrt{aC} \).
Conversely, let \( b \in \sqrt{aC} \). Then \( b^n = \sum_{i=1}^{r} a_i x_i \), with \( a_i \in a, x_i \in C \). Then \( A[x_1, ..., x_r] \) is a finite module over \( A \). Since \( b^n A[x_1, ..., x_r] \subset aA[x_1, ..., x_r] \). It follows that the multiplication by \( b^n \) behave like a matrix on \( A[x_1, ..., x_r] \) with entries in \( a \). Hence \( b^n \) satisfies the characteristic polynomial with coefficient in \( a \). It follows that \( b \) is integral over \( a \). \( \square \)
Remark

Keep the notation as above, let $f(x)$ be an integral polynomial of $b \in B$ and $p(x)$ be its minimal polynomial over $K$. We remark that there is NO notion of ”minimal integral polynomial” in general because the division algorithm doesn’t holds in $A$. However, if $A$ is UFD, then by Gauss lemma, we have $p(x)|f(x)$ not only in $K[x]$ but also in $A[x]$. Hence the minimal polynomial is integral.
Lemma

Keep the notation as above, the minimal polynomial of \( b \in B \) is in \( A[x] \). If \( b \in B \) is integral over \( a \triangleleft A \), i.e. the integral polynomial has coefficients in \( a \), then the minimal polynomial of \( b \in B \) is in \( \sqrt{a}[x] \).
Proof. Assume now $b$ is integral over $a$ with minimal polynomial $p(x)$. Take a splitting field of $p(x)$, say $L/K$. And let $b = b_1, \ldots, b_n$ be conjugates of $b$. Then they satisfy $f(x)$ as well. Thus $b_i$ is integral over $a$. It’s not difficult to see that $p(x) = \prod_{i=1}^{n} (x - b_i)^{m_i}$ for some $m_i \geq 0$. The coefficient are combination of $b_i$ hence integral over $a$. Apply the above Lemma to the extension $A \subset K$, we have integral closure of $a$ is $\sqrt{a}$. Hence minimal polynomial is in $\sqrt{a}[x]$. \[\square\]
Let $A$ be an integrally closed domain with quotient field $K$. Given an extension $L/K$, one can consider $B$ to be the integral closure of $A$ in $L$. (We may assume that $L$ is algebraic over $K$, or even to be the splitting field of $B$.) Especially, in number theory, we usually consider a number field which is a finite extension over $\mathbb{Q}$. And let $\mathcal{O}$ be the domain of algebraic integers. The extension $\mathbb{Z} \subset \mathcal{O}$ justify our setup.
Proposition

Let $A$ be an integrally closed domain with quotient field $K$. Given a normal extension $L/K$, one can consider $B$ to be the integral closure of $A$ in $L$. Let $\mathfrak{p} \in \text{Spec} A$, then prime ideals in $B$ lying over $\mathfrak{p}$ are conjugate. That is, for $q_1, q_2 \in \text{Spec} B$ lying over $\mathfrak{p}$, there is $\sigma \in \text{Aut}_K L$ such that $\sigma(q_1) = q_2$. 
Proof.
We will only prove this under the assumption that \( B \) is finitely
generated over \( A \). (Then we may assume that \([L : K]\) is finite).
If \( q_2 \neq \sigma_j(q_1) \) for all \( j \) then \( q_2 \not\subset \sigma_j(q_1) \) for all \( j \).

claim. there is \( x \in q_2 \) such that \( x \not\in \sigma_j(q_1) \) for all \( j \). We leave this
claim as an exercise.

Let \( y = \prod_{\sigma_j \in \text{Aut}_K L} \sigma_j(x) \). Then \( y \) is invariant under \( \text{Aut}_K L \). We
may assume that \( y^{p^l} \) is separable over \( K \) for some \( l \geq 0 \). (If
\( \text{char}(K)=0 \), then \( l = 0 \).) Let \( S \) be the separable closure of \( K \) in \( L \).
Then \( S \) is Galois over \( K \) with \( \text{Aut}_K S = \text{Aut}_K L \) (cf. Thm. 12 of
lecture 1). Hence \( y^{p^l} \in K \). One notice that \( B \cap K = A \). It follows
that \( y^{p^l} \in A \). And then \( y \in K \) is integral over \( A \). Therefore,
\( y \in A \). We Clearly, \( y = x^{y/x} \in q_2 \). Hence \( y \in A \cap q_2 = p \subset q_1 \).
Hence \( \sigma_j(x) \in q_1 \) for some \( j \). This leads to a contradiction. \( \square \)
Corollary

Keep the notation as above. Assume furthermore that $B$ is finitely generated over $A$. Then for $\mathfrak{p} \in \text{Spec} A$, there are only finitely many prime ideal in $B$ lying over $\mathfrak{p}$. And any two of them are ”conjugate” to each other.
Proof.
Let \( L \) be the splitting field of \( B \) over \( K \). One sees that \( L/K \) is finite. Let \( C \) be the integral closure of \( A \) in \( L \). Clearly, \( A \subset B \subset C \). We know that prime ideal in \( C \) lying over \( \mathfrak{p} \) is conjugate to each other. Since the Galois group is finite. There are only finitely many prime ideals. Restrict to \( B \), then there are only finitely many prime ideals in \( B \) lying over \( \mathfrak{p} \). \( \square \)
Theorem (Going down theorem)

Keep the notation as above, i.e. $B$ is an domain integral over an integrally closed domain $A$. If there are $p_2 \subset p_1 \in \text{Spec}A$ and $q_1$ in $B$ lying over $p_1$. Then there is $q_2 \subset q_1 \in \text{Spec}B$ lying over $p_2$. 
Proof.
Let $L$ be the normal closure of $B$ over $K$ and $C$ be the integral closure of $A$ in $L$. It’s clear that $C$ is integral over $B$. There is a prime ideal $\mathfrak{q}_1$ in $C$ lying over $q_1$. And there is a prime ideal $\mathfrak{p}_2$ in $C$ lying over $p_2$. By Going up theorem, there is a prime ideal $\mathfrak{r}_1' \supset \mathfrak{r}_2$ in $C$ lying over $p_1$. Therefore, there is $\sigma \in \text{Aut}_K L$ such that $\sigma(\mathfrak{r}_1) = \mathfrak{r}_1'$. Then $\sigma^{-1}(\mathfrak{r}_2) \subset \mathfrak{r}_1$. Let $q_2 := \sigma^{-1}(\mathfrak{r}_2) \cap B$. Then we are done.
We close this section by recall

**Theorem (Noether normalization theorem)**

Let $R$ be a finitely generated domain over a field $k$. Let $r$ be the transcendental degree of $R$ over $k$. Then there exists $y_1, ..., y_r$ in $R$, algebraically independent over $k$, such that $R$ is integral over $k[y_1, ..., y_r]$. 
Let $F$ be the field of quotients of $R$. Then $r$ is defined to be the transcendental degree of $F$ over $k$. Let first consider the case $r = 1$ and see what could be the problem. If $r = 1$, then we can pick $y \in R$ which is transcendental over $k$. The hope is to show that $x \in R$ is integral over $k[y]$. However, all we know so far is $x^n + a_{n-1}x^{n-1} + \ldots + a_0 = 0$ for some $a_i = \frac{q_i(y)}{p_i(y)} \in k(y)$. Eliminate the denominators, we get

$$f_n(y)x^n + \ldots + f_0(y) = 0,$$

which is not enough to show that $x$ is integral over $k[y]$. 

(*
A possible way out is to consider $z := y - x^m$ for some $m \gg 0$, e.g. $m > n$. Then the equation $*$ is now $cx^{md+i} + g(x, z) = 0$, with $c \in k$, $d = \max \{\deg_y(f_i(y))\}$ and $\deg_x g(x, z) \leq (d - 1)m + i < dm$. Hence $x$ is integral over $k[z]$. More generally, if $x_1, \ldots, x_t$ is a set of generator of $R$ over $k$ and $r = 1$. We can pick $m \gg 0$ so that it normalize $x_i$ simultaneously. Finally, by induction on $r$. We are able to prove the theorem. We leave the induction step to the readers.
The main object in algebraic geometry is algebraic variety. One can consider it as zero locus of a set of polynomial, roughly. To set it up, let’s first fix an algebraically closed field $k$. The affine $n$-space over $k$, denoted $\mathbb{A}^n_k$, is the set of all $n$-tuples. To study $\mathbb{A}^n$, the polynomial ring $A := k[x_1, .., x_n]$ is a convenient tool. They are closely connected via the following operation:
1. Given a set of polynomials $T$, one can define $\mathcal{V}(T)$, the common zero locus of $T$. We call such $\mathcal{V}(T)$ an algebraic set.

2. Given a subset $Y$ of affine space, one can define $\mathcal{I}(Y)$ which consists of polynomials vanish along $Y$. It's immediate that $I(Y)$ is an ideal.

We remark that $\mathcal{V}(T) = \mathcal{V}(\langle T \rangle)$, where $\langle T \rangle$ denotes the ideal generated by $T$. 

These two operations give connection between ideals and algebraic sets. It’s not difficult to see that one can define a topology on $\mathbb{A}^n$ with algebraic sets as closed sets. This topology is called the Zariski topology. Can one also construct a topology on the algebraic side? The answer is yes, with some extra care.
To see these, one can verify the following:

**Proposition**

*Keep the notation as above. We have the following:*

1. $\mathcal{V}(0) = \mathbb{A}^n$.
2. $\mathcal{V}(A) = \emptyset$.
3. $\mathcal{V}(I_1) \cup \mathcal{V}(I_2) = \mathcal{V}(I_1I_2)$.
4. $\cap \mathcal{V}(I_\alpha) = \mathcal{V}(\cup I_\alpha)$.
One notices that different ideals might give the same algebraic set, for example, the ideal \((x)\) and \((x^3)\) do. Among all ideals defining the same algebraic set, there is a maximal one, the *radical ideal*. So we have an one-to-one correspondence between radical ideals and algebraic sets.
Moreover, we have the following

**Theorem (Hilbert’s Nullstellensatz, weak form)**

*Every maximal ideal of $A = k[x_1, \ldots, x_n]$ is of the form $(x_1 - a_1, \ldots, x_n - a_n)$.*
Proof.
Let \( \mathfrak{m} \) be a maximal ideal of \( A \), we consider \( R := A/\mathfrak{m} \). \( R \) is clearly a finitely generated \( k \)-algebra. By Noether normalization theorem, there exists \( y_1, \ldots, y_r \in R \) such that \( R \) is integral over \( k[y_1, \ldots, y_r] \). Since \( R \) is a field, so is \( k[y_1, \ldots, y_r] \). This is possible only when \( r = 0 \). So \( R \) is integral over \( k \), hence algebraic over \( k \). But \( k \) is algebraically closed. So \( R = k \).
\( \square \)
**Theorem (Hilbert’s Nullstellensatz)**

Let $k$ be an algebraically closed field and $A = k[x_1, \ldots, x_n]$ be the polynomial ring. Let $\mathfrak{a}$ be an ideal in $A$, then

$$\mathcal{I}(\mathcal{V}(\mathfrak{a})) = \sqrt{\mathfrak{a}}.$$

**Corollary**

There is an one-to-one correspondence between algebraic sets and radical ideals. Furthermore, the algebraic set is irreducible (resp. a point) if and only if its ideal is prime (resp. maximal).
Definition

An algebraic set $X$ is irreducible if it can’t be written as union of two algebraic sets in a non-trivial way. More precisely, if $X = X_1 \cup X_2$ with $X_i$ being algebraic sets, then either $X = X_1$ or $X = X_2$.

An affine variety is an irreducible algebraic set in $\mathbb{A}^n$. An open subset of an affine variety is a quasi-affine variety.
Since $A$ is Noetherian, it’s easy to see that every algebraic set can be written as finite union of affine varieties. (This is basically what primary decomposition does). For an algebraic set $X$, it has the induced Zariski topology. It’s easy to see that it has descending chain condition for closed subsets, i.e. for any sequence $Y_1 \supseteq Y_2 \supseteq \ldots$ of closed subsets, there is an integer $r$ such that $Y_r = Y_{r+1} = \ldots$. A topological space is called Noetherian if it has d.c.c for closed subsets.

With the correspondence in mind, we can define the concept of dimension geometrically and algebraically.
Definition

For a Noetherian topological space $X$, the dimension of $X$, denoted $\dim X$, is defined to be the supremum (=maximum) of the length of chain of closed subvarieties.
For an affine variety $X \subset \mathbb{A}^n$, the polynomial functions $A$ restrict to $X$ is nothing but the homomorphism $\pi : A \to A/I(X)$. The ring $A/I(X)$ is called the coordinate ring of $X$, denoted $A(X)$. One can recover the geometry of $X$ from $A(X)$ by considering $\text{Spec}(A(X))$, which consist of prime ideals in $A(X)$. One can give the Zariski topology on $\text{Spec}(A(X))$ which is closely related to the Zariski topology on $X$. This is actually the construction of affine scheme. And affine variety can be viewed as a nice affine scheme.
Exercise

The coordinate ring of an affine variety is a domain and a finitely generated $k$-algebra. Conversely, a domain which is a finitely generated $k$-algebra is a coordinate ring of an affine variety.
One can also similarly define the *Krull dimension* or simply dimension to be the supremum of length of chain of prime ideals of a ring. It’s easy to see that for an algebraic set $X$, then

$$\dim X = \dim A(X).$$

However, it’s not trivial to prove that $\dim \mathbb{A}^n = n$. 
A projective $n$-space, denoted $\mathbb{P}^n$ is defined to be the set of equivalence classes of $(n + 1)$ tuples $(a_0, \ldots, a_n)$, with not all zero. Where the equivalent relation is $(a_0, \ldots, a_n) \sim (\lambda a_0, \ldots, \lambda a_n)$ for all $\lambda \neq 0$. We usually write the equivalence class as $[a_0, \ldots, a_n]$ or $(a_0 : \ldots : a_n)$.

One can first consider $\mathbb{P}^n$ as a quotient of $\mathbb{A}^{n+1} - \{(0, \ldots, 0)\}$. Let $\pi : \mathbb{A}^{n+1} - \{(0, \ldots, 0)\} \rightarrow \mathbb{P}^n$ be the quotient map. And we can topologize $\mathbb{P}^n$ by the quotient topology of Zariski topology. Then one sees that for a closed set $Y \subset \mathbb{P}^n$, $\pi^{-1}(Y)$ corresponds to a homogeneous ideal $I \triangleleft k[x_0, \ldots, x_n]$. 
We have the similar correspondence between projective algebraic sets and homogeneous radical ideals. There is an ideal need to be excluded, the *irrelevant maximal ideal*, \((x_0, \ldots, x_n)\).

Another important description is to give \(\mathbb{P}^n\) an open covering of \(n + 1\) copies of \(\mathbb{A}^n\). It follows that every projective variety can be covered by affine varieties.

To this end, we can simply consider

\[
\iota_j : \mathbb{A}^n \to \mathbb{P}^n \ \text{by} \ \iota_j(a_1, \ldots, a_n) = [a_1, \ldots, a_{j-1}, 1, a_j, \ldots, a_n].
\]

On the other hand, let \(H_j\) be the hyperplane \(x_j = 0\) in \(\mathbb{P}^n\). Then we have

\[
p_j : \mathbb{P}^n - H_j \to \mathbb{A}^n \ \text{by} \ p_j[a_0, \ldots, a_n] = (a_0/a_j, \ldots, a_{j-1}/a_j, a_{j+1}/a_j, \ldots, a_n/a_j).
\]
Example

We have seen that an elliptic curve $E$ can be maps to $\mathbb{C}^2$ by the Weierstrass functions. Compose with $\nu_2$, we have a map $\varphi : E \to \mathbb{P}^2$. The defining equation in $\mathbb{C}^2$ is $y^2 = 4x^3 - g_2x - g_3$. While the defining equation in $\mathbb{P}^2$ is the homogenized equation $y^2z = 4x^3 - g_2xz^2 - g_3z^3$.
In general, the equations in affine spaces and projective spaces are corresponding by *homogenization* and *dehomogenization*. By a *variety*, we mean affine, quasi-affine, projective or quasi-projective variety. (More generally, an abstract variety can be defined as an *integral separated scheme of finite type over an algebraically closed field* $k$).