From Algebraic to Weak Subintegral Extensions in Algebra and Geometry

Marie A. Vitulli

University of Oregon
Eugene, OR 97403

August 8, 2014
“My entire career has been devoted to increasing the number of African American women in mathematics and mathematics-related careers.”
To Greeks, algebra is essentially “geometric.”

Greek geometry and number theory were sophisticated but Greek algebra was weak.

Calculations with magnitudes and their relations rather than numbers.

They created and intersected auxiliary curves to solve algebraic problems.
Muhammad bin Musa al-Khwārizmī (c. 780 - c. 850) was a Persian mathematician, astronomer and geographer from a district not far from Baghdad. Under the region of Caliph al-Ma’mūhn he became a member of the “House of Wisdom.”

His book *al-jabr w al-muqabala* describes techniques to solve quadratic equations, which he classified into 5 types.

**Figure:** al-Khwārizmī
Completing the Square 1

Solve (in modern notation)

\[ x^2 + 10x = 39. \]
Completing the Square 2

Equivalently, solve

$$(x + 5)^2 = 39 + 25 = 64.$$
General Polynomial Equations

By late 16th and early 17th century focus shifted to solvability of polynomial equations with $l$ coefficients that weren’t specific numbers. If wasn’t until much later that mathematicians were to consider nonspecific coefficients that weren’t necessarily real numbers.
Study of General Polynomial Equations 2

How do we find the roots of a polynomials, preferably an exact solution in term of radicals?

- Solution in radicals given for cubic (degree 3) equation published by Cardano in 1545; known earlier by del Ferro and Tartaglia.
- Formula in radicals for roots of quartic (degree 4) equations given by Ferrari.
- In 1771 Joseph Lagrange gave a unifying method for producing roots of polynomials of degree at most 4.
- In 1824 Norwegian mathematician Niels Henrik Abel that the roots of a general quintic (degree 5) polynomial cannot be expressed as a finite number of radicals in the coefficients.
In his book “Geometry” (1637) René Descartes used fully symbolic notation.

- $x, y, z, \ldots$ were used to denote variables
- $a, b, c, \ldots$ were used to denote parameters
- Homogeneity of algebraic expressions was no longer needed
The German mathematician Carl Friedrich Gauss made significant contributions to many fields, including number theory, algebra, statistics, analysis, differential geometry, geophysics, astronomy, and optics. He is sometimes referred to as “The Prince of Mathematics.”
In his 1797 dissertation Gauss gave the first of four proofs of what is today known as the “Fundamental Theorem of Algebra (FTA)”, namely, that every polynomial with real or complex coefficients can be factored into linear factors over the complex numbers.

**Theorem (FTA 1)**

Every polynomial \( f(x) = x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n = 0 \) with real coefficients can be factored into linear and quadratic factors over the real numbers.
All of the results mentioned up to this point consider polynomials with rational, real, or complex coefficients.

Both Abel and Galois had an understanding of what we now call a “field”, that is, an algebraic structure in which you can add, subtract, multiply, and divide. In his memoir Galois states:

“one can agree to consider as rational every rational function of a certain number of quantities regarded as known a priori,”

and he describes the process of adjoining a new quantity to a known field of quantities. All fields they considered contained the field of rational numbers, so had characteristic 0. The finite field $F_p = \mathbb{Z}/p\mathbb{Z}$ and other finite fields containing $F_p$, were also considered by Galois. These are fields of characteristic $p$. 

M. A. Vitulli

Algebraic to Subintegral Extensions
Algebraic Elements and Extensions

**Definition**

Let \( K \subset L \) be fields and \( x \in L \). We say \( x \) is **algebraic** over \( K \) if there exist a positive integer \( n \) and \( a_1, \ldots, a_n \in K \) such that

\[
x^n + a_1 x^{n-1} + \cdots + a_{n-1} x + a_n = 0.
\]

We say that \( K \subset L \) is **algebraic extension** if every \( x \in L \) is algebraic over \( K \). If \( x \in L \) is not algebraic over \( K \) we say \( x \) is **transcendental** over \( K \). If \( K \subset L \) is not an algebraic extension we say it is a **transcendental extension**.
Some Algebraic and Transcendental Extensions

The following extensions of fields are algebraic.

- \( \mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\} \)
- \( F_2 \subset F_2[X]/(X^3 + X + 1) \)

The next list consists of transcendental extensions.

- \( \mathbb{Q} \subset \mathbb{Q}(\pi) \)
- \( \mathbb{Q} \subset \mathbb{Q}(X) = \{F(X)/G(X) \mid F(X), G(X) \in \mathbb{Q}[X]\} \)
Algebraic Closure of a Field

**Definition**

Let $K \subset L$ be an extension of fields. We define the **algebraic closure** $\overline{K}_L$ of $K$ in $L$ to be

$$\overline{K}_L = \{x \in L \mid x \text{ is algebraic over } K\}.$$  

We say **$K$ is algebraically closed in $L$** if $K = \overline{K}_L$.

It is well known that $\overline{K}_L$ is a field and is algebraically closed in $L$.

**Definition**

We say a field $K$ is **algebraically closed** if there does not exist an algebraic extension of fields $K \subsetneq L$. The **algebraic closure** $\overline{K}$ of a field $K$ is an algebraic field extension of $K$ that is algebraically closed.
We now consider commutative rings (so $ab = ba$) with (multiplicative) identity $1$. The rings $\mathbb{Z}$ and $\mathbb{Q}[X]$ are examples of commutative rings with $1$.

**Definition**

Let $A \subset B$ be an extension of rings and $x \in B$. We say $x$ is **integral** over $A$ if there exist a positive integer $n$ and $a_1, \ldots, a_n \in A$ such that

$$x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n = 0.$$  

We say that $A \subset B$ is **integral extension** if every $x \in B$ is integral over $A$. 
Examples of Integral and Nonintegral Extensions

The following are integral extensions of rings.

- \( \mathbb{Z} \subset \mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\} \)
- \( \mathbb{R} \subset \mathbb{R}[X]/(X^2 + 1) \)

The following extensions of rings are not integral.

- \( \mathbb{Z} \subset \mathbb{Z}[\pi] \)
- \( \mathbb{C} \subset \mathbb{C}[X] \)
Suppose $A \subset B$ is an integral extension of rings. Then,

- every prime ideal $P$ of $A$ is the contraction $Q \cap A$ of a prime ideal $Q$ of $B$ (Lying Over), and
- for any given prime ideal $P$ of $A$, there are no containment relations among the primes of $B$ that lie over $P$ (Incomparability).

We next present the ring analog of the relative notion of the algebraic closure of a field in an extension field.
Integral Closure of $A$ in $B$

**Definition**

Suppose that $A \subset B$ is an extension of rings. The set

$$\overline{A}_B = \{x \in B \mid x \text{ is integral over } A\}$$

is called **integral closure of $A$ in $B$**. We say that $A$ is **integrally closed in $B$** if $A = \overline{A}_B$.

Analogous to the field case, $\overline{A}_B$ is a subring of $B$ and is integrally closed in $B$. 
Normal Domains and Normalization

**Definition**

We say that an integral domain $A$ is **normal** provided that $A$ is integrally closed in quotient field $K$. We define the **normalization** $\overline{A}$ of $A$ to be the integral closure of $A$ in its quotient field $K$.

We point out that any unique factorization domain is normal. In particular, $\mathbb{Z}$ and $\mathbb{Q}[X]$ are normal integral domains.
Integral Closure of an Ideal

**Definition**

Let $I \subseteq A$ be an ideal of a ring $A$. We say an element $x \in A$ is **integral over $I$** provided that there exist a positive integer $n$ and elements $a_k \in I^k (k = 1, \ldots, n)$ such that

$$x^n + a_1 x^{n-1} + \cdots + a_{n-1} x + a_n = 0.$$ 

We define the **integral closure of $I$** to be the set

$$\overline{I} = \{ x \in A \mid x \text{ is integral over } I \}.$$ 

We say that $I$ is **integrally closed** if $I = \overline{I}$.

It is well known that $\overline{I}$ is an integrally closed ideal of $A$. 
The Exponent Set of a Monomial Ideal

Suppose that $I \subset K[X_1, \ldots, X_n]$ is a monomial ideal, that is, $I$ is generated by monomials. For a tuple $\alpha = (a_1, \ldots, a_n)$ of nonnegative integers we let $X^\alpha = X_1^{a_1} \cdots X_n^{a_n}$.

Define the exponent set of $I$ to be the set

$$\Gamma(I) = \{ \alpha \in \mathbb{N}^n \mid X^\alpha \in I \}$$

and the Newton Polyhedron of $I$ to be the set

$$NP(I) = \text{conv}(\Gamma(I)),$$

where $\text{conv}(S)$ stands for convex hull of a subset $S \subset \mathbb{R}^n$. 
The Integral Closure of a Monomial Ideal

It is well known that the integral closure $\overline{I}$ of a monomial ideal $I$ is again a monomial ideal with exponent set

$$\Gamma(\overline{I}) = \overline{\Gamma(I)} := \{ \alpha \in \mathbb{N}^n \mid m\alpha \in \sum_{i=1}^{m} \Gamma(I) \exists m \geq 1 \}.$$  

Furthermore, we know that

$$\Gamma(\overline{I}) = \text{NP}(I) \cap \mathbb{N}^n.$$
Example. In the polynomial ring $K[X, Y]$ over the field $K$ consider the monomial ideal $I = (X^4, X^3Y^2, Y^3)$ and its integral closure $\bar{I} = (X^4, X^3Y, X^2Y^2, Y^3)$. 
Definition

An ideal $I$ of a ring $A$ is said to be **normal** if $I^k$ is integrally closed for all $k \geq 1$.

Notice that $(X, Y) \subset K[X, Y]$ is a normal ideal.

It turns out that one doesn’t have to test all positive powers of a monomial ideal to establish normality.

**Theorem (Reid-Roberts-V)**

*Let $I \subset K[X_1, \ldots, X_n]$ be a monomial ideal. If $I^k$ is integrally closed for $k = 1, \ldots, n - 1$, then $I$ is normal.*
Some Classes of Normal Ideals

This result enables us to produce classes of normal and nonnormal monomial ideals in $K[X_1, X_2]$ and $K[X_1, X_2, X_3]$. For a tuple $\lambda = (\lambda_1, \ldots, \lambda_n)$ of positive integers define

$$I(\lambda) = (X_1^{\lambda_1}, \ldots, X_n^{\lambda_n}).$$

**Theorem (Reid-Roberts-V)**

Let $\lambda = (\lambda_1, \lambda_2, \lambda_3)$ be an ordered triple of positive integers. If $\gcd(\lambda_1, \lambda_2, \lambda_3) > 1$, then $I(\lambda) \subset K[X_1, X_2, X_3]$ is normal.

Here is another class found by a student of mine.

**Theorem (H. Coughlin, 2004)**

Let $\lambda = (j, j + 1, j + 2)$ for $j \geq 2$. The monomial ideal $I(\lambda) \subset K[X_1, X_2, X_3]$ is normal if and only if $j$ is even.
Algebraic Varieties

Classically, an **algebraic variety** was defined to be the set of common zeroes of a system of polynomial equations over the real or complex numbers. Today, these are called **affine algebraic sets** and the fields of coefficients can be arbitrary algebraically closed fields. Abstract algebraic varieties were defined by patching together these affine algebraic sets.
Affine Algebraic Sets and Affine Coordinate Rings

To an affine algebraic set

\[ V = Z(F_1(X_1, \ldots, X_n), \ldots, F_s(X_1, \ldots, X_n)) \subset K^n \]

we associate its **affine coordinate ring**

\[ \Gamma(V) = K[X_1, \ldots, X_n]/I(V) := K[x_1, \ldots, x_n], \text{ where} \]

\[ I(V) = \{ F(X_1, \ldots, X_n) \in K[X_1, \ldots, X_n] \mid F(a) = 0 \ \forall a \in V \} \]

and \( x_i = X_i + I(V) \).
Affine $n$-space $K^n$ is a topological space where the closed subsets are the affine algebraic sets; this is the Zariski topology.

If a nonempty algebraic set can not be expressed as the union of two proper closed subsets it is irreducible.

$V$ is irreducible if and only if $I(V)$ is a prime ideal of $K[X_1, \ldots, X_n]$. 
The **dimension** of an affine algebraic variety $V$ is the maximal length of a chain of irreducible closed subsets $V_0 \subset V_1 \subset \cdots \subset V_n$.

Since irreducible closed subsets of $V$ correspond to prime ideals of $\Gamma(V)$, the dimension of $V$ equals the **Krull dimension** of $\Gamma(V)$, which is the maximal length of a chain of prime ideals of $\Gamma(V)$.

A **curve** is a 1-dimensional variety and a **surface** is a 2-dimensional variety.
The Ordinary Double Point

This plane curve has a singularity at the origin, called an ordinary double point or node. Its affine coordinate ring \( \mathbb{C}[X, Y]/(Y^2 - X^3 - 3X^2) := \mathbb{C}[x, y] \) is an integral domain that is not normal. Indeed, \( \mathbb{C}[x, y] = \mathbb{C}[y/x] \).

Figure: \( Z(Y^2 - X^3 - 3X^2) \)
Suppose that $C$ is an irreducible affine curve and let $A$ denote its affine coordinate ring. Then, $\overline{A}$ is the affine coordinate ring of an irreducible affine curve $\widetilde{C}$ and the associated map $\pi: \widetilde{C} \to C$ is a surjective closed mapping with finite fibers. This map is called the \textit{normalization} of $C$. The curve $\widetilde{C}$ is nonsingular.

\textbf{Example}

Let $C = Z(Y^2 - X^3 - 3X^2) \subset \mathbb{C}^2$ so that $\widetilde{C} = \mathbb{C}^1$ and

$$\pi: \widetilde{C} \to C \text{ is given by } \pi(t) = (t^2 - 3, t(t^2 - 3)).$$

Notice that $\pi$ is 1-1 except that $\pi^{-1}(0, 0) = \{\pm \sqrt{3}\}$. 
**Subintegral Extensions**

**Definition**

An extension of rings $A \subset B$ is **subintegral** if

1. $B$ is integral over $A$;
2. for each prime ideal of $A$ there is a unique prime ideal of $B$ lying over it; and
3. the residue field extensions are isomorphisms.

These were first studied and called **quasi-isomorphisms** by Silvio Greco and Carlo Traverso. Richard Swan was first to call them subintegral extensions circa 1980.
The Cusp

This plane curve has a singularity at the origin called a cusp. Consider its affine coordinate ring and its normalization
\[ \mathbb{C}[X, Y]/(X^3 - Y^2) =: \mathbb{C}[x, y] \subset \mathbb{C}[y/x] = \mathbb{C}[x, y]. \]

This is a subintegral extension, since the nonzero primes of \( \mathbb{C}[x, y] \) are of the form \((x - a, y - b)\), where \(a^3 = b^2\), and the unique prime of \( \mathbb{C}[y/x] \) lying over \((x - a, y - b)\) is \((y/x)\) if \(a = 0\) and \((y/x - b/a)\) if \(a \neq 0\).

Figure : \( Z(X^3 - Y^2) \)
Weakly Subintegral Extensions

**Definition**

An extension of rings \( A \subset B \) is **weakly subintegral** if

1. \( B \) is integral over \( A \);
2. for each prime ideal of \( A \) there is a unique prime ideal of \( B \) lying over it; and
3. the residue field extensions are purely inseparable.

Recall that \( F_p(X^p) \subset F_p(X) \) is a purely inseparable extension of fields; this is a weakly subintegral extension of rings.

If \( \mathbb{Q} \subset A \) the notions of subintegral and weakly subintegral extensions coincide; we will mainly be concerned with this case and I will sometimes blur the distinction.
Local Gluing

Suppose that \( A \subset B \) is an integral extensions of rings and that \( A \) is local with unique maximal ideal \( \mathfrak{m} \). Then, all of the maximal ideals of \( B \) lie over \( \mathfrak{m} \). Let \( R(B) \) denote the Jacobson radical of \( B \), that is, the intersection of the maximal ideals of \( B \). Consider the subring \( A' = A + R(B) \). This ring is called the gluing of \( A \) in \( B \) over \( \mathfrak{m} \).

**Theorem**

Let \( A \subset A' \subset B \) be as above. Then,

- \( A' \) is local with unique maximal ideal \( \mathfrak{m}' = R(B) \); and
- the induced map \( A/\mathfrak{m} \to A'/\mathfrak{m}' \) is an isomorphism.

This notion of gluing was introduced by Traverso. A notion of weak gluing was introduced earlier by Andreotti and Bombieri in the context of schemes, which are generalizations of algebraic varieties.
A ring is said to be **reduced** if $x^n = 0$ in $A \Rightarrow x = 0$.

**Definition**

For an integral extension $A \subset B$ we define the **seminormalization** $+_BA$ of $A$ in $B$ by

$$+_BA = \{b \in B \mid b_P \in A_P + R(B_P), \forall \text{ primes } P \subset A\}.$$

By the **seminormalization** $+_A$ of a reduced ring $A$ whose total quotient ring $K$ is a product of fields, we mean its seminormalization in $\overline{A}$, the normalization of $A$.

Notice that the seminormalization of $A$ in $B$ is obtained by gluing over all the prime ideals of $A$. This concept was introduced by Traverso.
Seminormal Extension

**Definition**

Let $A \subset B$ be an integral extension of rings. We say that $A$ is **seminormal** in $B$ (or that the extension is seminormal) provided that $A = \frac{+}{B}A$. We say a reduced ring whose total ring of quotients is a product of fields is **seminormal** if $A = +A$.

Notice that the result on local gluing implies that the extension $A \subset \frac{+}{B}A$ is subintegral. We point out that $A$ is seminormal in $B$ if and only if there does not exist an intermediate ring $C$ such that $A \subsetneq C$ is subintegral.
Hamann’s Criterion

Let $A \subset B$ be an arbitrary integral extension. $A$ is seminormal in $B$ if and only if

$$b \in B, b^2, b^3 \in A \Rightarrow b \in A$$

Example

Let $K$ be a ring and $X$ an indeterminate. Then,

- $K[X^2, X^3] \subset K[X]$ is a subintegral extension.
- $K[X^2, X^3] \subset K[X]$ is not a seminormal extension.
- $K[X^2] \subset K[X]$ is a seminormal extension when $K$ is a field.
The Ordinary Double Point is Seminormal

Example

Consider the affine coordinate ring of the ordinary double point $\mathbb{C}[X,Y]/(Y^2 - X^3 - 3X^2) := \mathbb{C}[x,y]$ and its normalization

$$\mathbb{C}[x,y] \subset \overline{\mathbb{C}[x,y]} = \mathbb{C}[y/x].$$

The maximal ideals of $\mathbb{C}[x,y]$ are of the form $(x-a, y-b)$, where $b^2 = a^3 + 3a^2$. Note that $(y/x - \sqrt{3})$ and $(y/x + \sqrt{3})$ in $\mathbb{C}[y/x]$ both lie over $(x, y)$ in $\mathbb{C}[x,y]$. Since

$$(y/x - \sqrt{3}) \cap (y/x + \sqrt{3}) = ((y/x)^2 - 3)\mathbb{C}[x/y] = (x,y)\mathbb{C}[x,y]$$

and all other points on the curve are nonsingular, $\mathbb{C}[x,y]$ is seminormal.
Clarification

Let $A \subset B$ be an integral extension.

- $A$ is seminormal in $B \iff A$ DOES NOT admit any proper subintegral extension in $B$ (so $A$ is “subintegrally closed” in $B$).

- Subintegral extensions and seminormal extensions are complementary notions.
Traverso’s Characterization

Theorem (Traverso, 1970)

Let $A \subset B$ be an integral extension of rings. Then,

1. $A \subset \frac{+}{B}A$ is a subintegral extension.
2. $\frac{+}{B}A \subset B$ is a seminormal extension.
3. $\frac{+}{B}A$ is the unique largest subintegral extension of $A$ in $B$. 
Theorem (Leahy-V)

- If $A \subset B$ is a seminormal extension and $A$ is any multiplicative subset of $A$, then $S^{-1}A \subset S^{-1}B$ is seminormal.
- The operations of seminormalization and localization commute.
- $A$ is seminormal in $B \iff A_m$ is seminormal in $B_m$ for every maximal ideal $m$ of $A$.
- The local ring of an algebraic variety is seminormal if and only if its completion is seminormal.
Since there are no nontrivial seminormal extensions of fields there is little hope of giving an elementwise characterization of seminormality. Thus we switch gears at this point and talk about weakly subintegral extensions.

**Definition**

Let $A \subset B$ be an extension of rings and $b \in B$. We say $b$ is **weakly subintegral** over $A$ provided that $A \subset A[b]$ is a weakly subintegral extension.
Lemma (V)

Suppose that $K \subset L$ is an extension of fields and $x \in L$. Then, $x$ is weakly subintegral over $K$ $\iff$ $x$ is a common root of some monic polynomial $F(T) \in K[T]$ of positive degree $n$ and its first $\left\lfloor \frac{n}{2} \right\rfloor$ derivatives.

Theorem (V)

Let $A \subset B$ be an extension of rings and $x \in B$. Then, $x$ is weakly subintegral over $A$ $\iff$ there is some monic polynomial $F(T) \in A[T]$ of positive degree $n$ such that $x$ is a common root of $F(T)$ and its first $\left\lfloor \frac{n}{2} \right\rfloor$ derivatives.
New Criterion for Weak Subintegrality

Lemma (V)
Suppose that $K \subset L$ is an extension of fields and $x \in L$. Then, $x$ is weakly subintegral over $K \iff x$ is a common root of some monic polynomial $F(T) \in K[T]$ of positive degree $n$ and its first $\lfloor \frac{n}{2} \rfloor$ derivatives.

Theorem (V)
Let $A \subset B$ be an extension of rings and $x \in B$. Then, $x$ is weakly subintegral over $A \iff$ there is some monic polynomial $F(T) \in A[T]$ of positive degree $n$ such that $x$ is a common root of $F(T)$ and its first $\lfloor \frac{n}{2} \rfloor$ derivatives.