The Arithmetic Case in Commutative Algebra

Paul C. Roberts

September 24, 2010

Topics:

1. Background: The Arithmetic case in classical commutative algebra.

2. Some recent developments on questions in the Arithmetic case.

Some background in Commutative Algebra

The subject of Commutative Algebra arose from Algebraic Geometry and Number Theory. The basic idea was give a firm foundation for the algebraic part of the theory and to do it in a unified way.

Some background in Commutative Algebra

The subject of Commutative Algebra arose from Algebraic Geometry and Number Theory. The basic idea was give a firm foundation for the algebraic part of the theory and to do it in a unified way.

Here are two important motivating questions:

From Algebraic Geometry: Finding and studying sets of solutions to systems of polynomial equations over a field such as the field of Complex Numbers.

From Number Theory: factorization in fields of algebraic numbers.

Geometric Background:

We start with the polynomial ring $\mathbb{C}[x_1, \ldots, x_n]$ over the field of complex numbers. Hilbert showed that there is a correspondence between algebraic subsets of $\mathbb{C}^n$ and certain ideals of $\mathbb{C}[x_1, \ldots, x_n]$.

This gave a way of relating geometric ideas in an algebraic situation.

The ring $\mathbb{C}[x_1, \ldots, x_n]$ is *Noetherian*; that is, it has ascending chain condition on ideals. Much of Commutative Algebra is about extending geometric ideas to Noetherian rings.

Number Theory Background:

One of the origins from number theory is to extend unique factorization in the ring $\mathbb{Z}$ of integers to finite extensions of $\mathbb{Z}$ such as the Gaussian Integers $\mathbb{Z}[i]$. This is not always possible, but Kummer and others discovered that you can factor ideals uniquely as products of prime ideals.

(This is the source of the term "ideal". An ideal in a ring R is a subset I closed under addition and such that if $i \in I$ and $r \in R$ then $ri \in I$. An example is the set of multiples of a given element r_0 of R.)

These rings are also Noetherian, and are what I have called the Arithmetic case. More generally, one can have rings of polynomials over rings of algebraic integers and homomorphic images of these.

Local Rings

In the problems we consider we look at "local rings".

Example: The ring of rational functions defined locally at the origin. This is the ring R of functions $f(x_1, \ldots, x_n)/g(x_1, \ldots, x_n)$ where f and g are polynomials and $g(0, \ldots, 0) \neq 0$. R is a *local ring*; that is, it has a unique maximal ideal. In this case it consists of $f(x)/g(x)$ where $f(0) = 0$.

A *local ring* is a Noetherian ring with a unique maximal ideal.

In the remainder of the talk we will consider mostly local rings.

Dimension in Local Rings

Example In the local ring at the origin defined above, the maximal ideal (consisting of functions vanishing at the origin) is generated by $x_1, \ldots x_n$, since a polynomial vanishes at the origin if and only if its constant term is zero which is true if an only if it can be written

$$x_1 h_1(x) + \cdots + x_n h_n(x).$$

Dimension in Local Rings

Example In the local ring at the origin defined above, the maximal ideal (consisting of functions vanishing at the origin) is generated by $x_1, \ldots x_n$, since a polynomial vanishes at the origin if and only if its constant term is zero which is true if an only if it can be written

$$x_1 h_1(x) + \cdots + x_n h_n(x).$$

Let R be a local ring with maximal ideal $\mathfrak{m}$. A *system of parameters* for R is a sequence of elements $x_1, \ldots, x_d$ in $\mathfrak{m}$ such that

1. $\mathfrak{m}$ is the only prime ideal containing $x_1, \ldots, x_d$.
2. d is the smallest number for which a sequence satisfying (1) exists.

The number d is the *dimension* of R.

This does give n in the example above.

Completion

Example–the p-adic integers. Take a prime number p. The p-adic integers are the limit of

$$\cdots \to \mathbb{Z}/p^n\mathbb{Z} \to \cdots \mathbb{Z}/p^2\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}.$$

An element can be considered as a sequence of approximations modulo, p, modulo p^2, and so on. It can be represented

$$a_0 + a_1 p + a_2 p^2 + \cdots .$$

If R is a local ring with maximal ideal $\mathfrak{m}$, its *completion* is the limit

$$\cdots \to R/\mathfrak{m}^n \to \cdots R/\mathfrak{m}^2 \to R/\mathfrak{m}.$$

A local ring is *complete* if it is isomorphic to its completion.

The completion of the local ring of rational functions defined at the origin is the ring of power series in $x_1, \ldots x_n$.

The Cohen structure theorems.

Suppose R is a complete local ring of dimension d containing a field. Then R contains a subring S which is a power series ring over a field such that R is finite over S. This means that there is a finite set $\{r_1, \ldots r_t\}$ in R such that every element of R can be written as

$$s_1 r_1 + \cdots + s_t r_t$$

with $s_i \in S$.

This implies that R satisfies a lot of nice properties.

What about the arithmetic case, where R does not contain a field?

What about the arithmetic case, where R does not contain a field?

Many problems in Commutative Algebra are treated in three cases:

1. Characteristic zero: R contains a field of characteristic zero.
2. Positive characteristic: R contains a field of positive characteristic p for some prime number p.
3. Mixed characteristic: $R/\mathfrak{m}$ is a field of characteristic p for some p but p is not zero in R. This is the arithmetic case, and for many problems it is the most difficult.

The ring of Witt vectors.

The ring of Witt vectors can take the place of the field in the Cohen structure theorem.

Let k be a field of positive characteristic p. A Witt vector is a sequence $(a_0, a_1, \ldots)$ with a_i in k. Addition and multiplication are very complicated, but here is an example of how it works: we give the formula for addition in the first two components:

$$(a_0, a_1, \ldots) + (b_0, b_1, \ldots) = (a_0 + b_0,$$
$$a_1 + b_1 + \frac{(a_0^p + b_0^p) - (a_0 + b_0)^p}{p}, \ldots).$$

The ring of Witt vectors.

The ring of Witt vectors can take the place of the field in the Cohen structure theorem.

Let k be a field of positive characteristic p. A Witt vector is a sequence $(a_0, a_1, \ldots)$ with a_i in k. Addition and multiplication are very complicated, but here is an example of how it works: we give the formula for addition in the first two components:

$$(a_0, a_1, \ldots) + (b_0, b_1, \ldots) = (a_0 + b_0,$$
$$a_1 + b_1 + \frac{(a_0^p + b_0^p) - (a_0 + b_0)^p}{p}, \ldots).$$

As this stands it makes no sense

The ring of Witt vectors.

The ring of Witt vectors can take the place of the field in the Cohen structure theorem.

Let k be a field of positive characteristic p. A Witt vector is a sequence $(a_0, a_1, \ldots)$ with a_i in k. Addition and multiplication are very complicated, but here is an example of how it works: we give the formula for addition in the first two components:

$$(a_0, a_1, \ldots) + (b_0, b_1, \ldots) = (a_0 + b_0,$$
$$a_1 + b_1 + \frac{(a_0^p + b_0^p) - (a_0 + b_0)^p}{p}, \ldots).$$

As this stands it makes no sense–one has to derive the formulas in the case the a_i and b_i are integers, then use these formulas for a_i and b_i in a field of characteristic p.

This works because the binomial coefficients $\binom{p}{i}$ are divisible by p for i between 1 and $p-1$.

The Witt vectors are a "discrete valuation ring", that is they have a maximal ideal generated by p and every ideal is generated by a power of p.

Given this, we have a structure theorem as before. But there is a major difference. If R is a complete local ring containing a field and $x_1, \ldots, x_d$ is any system of parameters we can find a power series subring S where the variables are $x_1, \ldots x_d$.

If R has mixed characteristic, any subring S has to contain 1, so it has to contain $p \cdot 1 = p$. So we are forced to take p as part of the system of parameters.

The Witt vectors are a "discrete valuation ring", that is they have a maximal ideal generated by p and every ideal is generated by a power of p.

Given this, we have a structure theorem as before. But there is a major difference. If R is a complete local ring containing a field and $x_1, \ldots, x_d$ is any system of parameters we can find a power series subring S where the variables are $x_1, \ldots x_d$.

If R has mixed characteristic, any subring S has to contain 1, so it has to contain $p \cdot 1 = p$. So we are forced to take p as part of the system of parameters.

The Cohen structure theorem for mixed characteristic: If R is a complete local integral domain of mixed characteristic, then there is a subring S which is a power series ring $W[[x_2, \ldots, x_d]]$, where W is a ring of Witt vectors and R is a finite extension of S.

Some recent conjectures in the Mixed Characteristic Case

The problems we discuss here come ultimately from Serre's algebraic formulation of Intersection Theory. He gave a homological definition of the intersection multiplicity of two subschemes of a scheme in terms of Euler characteristics. He defined the intersection multiplicity for modules over a regular local ring.

Some recent conjectures in the Mixed Characteristic Case

The problems we discuss here come ultimately from Serre's algebraic formulation of Intersection Theory. He gave a homological definition of the intersection multiplicity of two subschemes of a scheme in terms of Euler characteristics. He defined the intersection multiplicity for modules over a regular local ring.

A local ring is *regular* if its maximal ideal can be generated by a system of parameters. This is the case for the ring of rational functions defined at the origin described above.

If R is a complete regular local ring containing a field, then R is a power series ring over a field.

If R does not contain a field, we need the condition that there is a system of parameters of the form $p, x_2, \ldots, x_d$ that generates the maximal ideal. This is the *unramified* case. It is often the ramified case that causes trouble.

The multiplicity is the degree of tangency, and it is crucial in enumerative geometry.

Serre proved several theorems for regular local rings that contain a field. We denote the intersection multiplicity of M and N by $\chi(M, N)$. The condition on M and N is that they intersect in only one point.

1. (Dimension) $\dim M + \dim N \leq \dim R$.
2. (Vanishing) If $\dim M + \dim N < \dim R$, then $\chi(M, N) = 0$.
3. (Nonnegativity) $\chi(M, N) \geq 0$.
4. (Positivity) If $\dim M + \dim N = \dim R$, then $\chi(M, N) > 0$.

He proved these in the equicharacteristic and unramified cases.

Here is the present situation on these conjectures.

1. **Question 1 (Dimension):** Proven by Serre.
2. **Question 2 (Vanishing):** Proven around 1985 (–,Gillet–Soulé).
3. **Question 3 (Nonnegativity):** Proven around 1996 (Gabber).
4. **Question 4 (Positivity):** Open.

Each of these developments involved new ingredients.

For Vanishing, new methods in Intersection Theory and K-theory, due to Fulton-MacPherson and others. The statements are independent of characteristic, but they use Cohen structure theorems.

For nonnegativity, Gabber used a version of resolution of singularities due to de Jong. Again the proof required special methods over a discrete valuation rings.

One curious fact about Gabber's proof is that he reduces at one point to the ramified case.

The question of resolution of singularities in positive characteristic is a major topic of research at present.

There are many other "Homological Conjectures". The most recent major advance was on the "Monomial Conjecture" of Mel Hochster, which states that if $x_1, \ldots, x_d$ is a system of parameters for a local ring, then for al $t > 0$,

$$x_1^t \cdots x_d^t \notin (x_1^{t+1}, \ldots, x_d^{t+1})$$

.

Consider the case where the x_i are variables in a polynomial ring, the ideal on the right is all polynomials with at least one of the x_i to at least the $t + 1$ power.

This has been known in equicharacteristic for some time. In 2002 Ray Heitmann proved it in dimension 3 in mixed characteristic.

The proof used (among other things) classical formulas that give the exact power of p that divides a given binomial coefficient.

The positive characteristic case.

In this case we have the Frobenius map.
The Frobenius map F is defined by $F(x) = x^p$. It is a ring homomorphism, working even better than the mixed characteristic case because the binomial coefficients are now 0.

An idea of how theorems can be proven using the Frobenius map:

If we had a counterexample, applying the Frobenius map gives worse and worse counterexamples, and eventually they are so bad we can prove they can't exist. This works, for example, for the Monomial Conjecture.

In Arithmetic Geometry, J.-M. Fontaine showed how to derive a positive characteristic ring from one of mixed characteristic, allowing him to reduce proofs of some facts in the mixed characteristic case on Galois representations to the positive characteristic case. Recently I have been working to apply this to the kind of problem we are discussing here.