Solving Algebraic Equations in Commutative Rings

Hideyuki Matsumura
Nagoya University

§ 0 Introduction

Let A be a commutative Ring, and let $f(x) = (f_1, \ldots, f_r)$ be a vector of polynomials in $X_1, \ldots, X_n$ with coefficients in A: $f_i(x) \in A[x_1, \ldots, x_n]$ $(1 \leqslant i \leqslant r)$. The problem is to find solutions of $f(x) = 0$ in A, i.e. to find $a_1, \ldots, a_n \in A$ such that $f_1(a) = \ldots = f_r(a) = 0$. When A is an algebraically closed field this problem leads to Algebraic Geometry, while when A = Z this is the problem of Diophantine Equations.

Let $\varphi : A \to B$ be a homomorphism of commutative rings, and let $f_i^{\varphi}(x)$ denote the polynomial obtained by applying ϕ to the coefficients of $f_i(x)$. Then $f(x) = 0$ has a solution in A $\Rightarrow f^{\varphi}(x) = 0$ has a solution in B. This is trivial (but useful to prove the unsolvability of $f(x) = 0$ in A. For instance if A = Z and B = Z/(n) then the solvability of $f^{\varphi}(x) = 0$ in Z/(n) can be checked by a finite number of trials, and if $f^{\varphi}(x) = o$ has no solution then $f(x) = 0$ has no solution.) The opposite implication is obviously false in general, but there are some important cases in which it is true. The main purpose of my talk is to explain this aspect of the problem in two cases. The first is the case of (simultaneous) linear equations, and the second is that of the Artin Approximation Theorems. Our discussion will show, hopefully, the importance of the operations of Localization, Completion and Henselization. In the following all rings are assumed to be commutative, to have a unit element 1 and to be different from $\{0\}$

§ 1. Linear Equations.

Local Rings

A ring A which has only one maximal ideal m is called a local ring; we say that (A, m) is a local ring, meaning that A is a local ring and m is its maximal ideal. As an example, let θ be the ring of holomorphic functions defined in neighbourhoods of the origin in C^n, where the domain of definition may vary from function to function, and two functions which coincide in a neighbourhood of the origin are considered equal. Then the set m consisting of functions vanishing at the origin is the only maximal ideal of θ, because if $f \in \theta$, $f \notin m$ then $1/f \in \theta$. Therefore θ is a local ring. (This ring can be identified with the ring of convergent power series in n variables $x_1, \ldots, x_n$ with coefficients in C, and is denoted by $C\{x_1, \ldots, x_n\}$.)

We can construct many local rings from an arbitrary ring by the following method.

---

*Text of a lecture delivered to the Singapore Mathematical Society on 23 February 1984.

Professor H. Matsumura is professor of mathematics at Nagoya University, Japan, since 1968, and has taught at Kyoto University, Columbia University, Brandeis University and University of Pennsylvania. He was a visiting professor at Munster, Germany, and Torino, Italy. He has made important contributions to algebraic geometry and commutative algebra. He is the author of the classic text, "Commutative algebra".

Localization Let A be a ring and P be a prime ideal (i.e. an ideal such that $x, y \in A - P$ implies $xy \notin P$). Put

$$A_P = \left\{ \frac{a}{s} \;/\; a \in A, s \in A - P \right\}$$

and if M is an A-module put

$$M_P = \left\{ \frac{x}{s} \;/\; x \in M, s \in A - P \right\}.$$

Here, two fractions $\frac{a}{s}$ and $\frac{a'}{s'}$ are defined to be equal iff there is $s'' \in A - P$ such that $s''(s'a - sa') = 0$; similarly in M_P. The A_P is a ring (by the usual formulas of sum and product of fractions) and M_P is an A_P – module. Moreover, A_P is a local ring. In fact, $m = \left\{ \frac{a}{s} \;/\; a \in P, s \in A - P \right\}$ is an ideal of A_P and the elements of $A_P - m$ are units (i.e. have their inverses) in A_P. Therefore m is the maximal ideal of A_P.

There is a natural map $M \to M_P$ which sends $x \in M$ to $\frac{x}{1} \in M_P$. We will write x_P for $\frac{x}{1}$. Then

$$x_P = 0 \Leftrightarrow \exists\ s \in A - P \text{ such that } sx = 0$$

$$\Leftrightarrow P \not\supset ann\,(x), \text{ where } ann(x) = \left\{ a \in A \mid ax = 0 \right\}.$$

We will use the following two properties of localization:

(I) Localization preserves exactness. Namely, if

$$\ldots \to L \to M \to N \to \ldots$$

is an exact sequence of A-modules, then the corresponding sequence of A_P – modules.

$$\ldots \to L_P \to M_P \to N_P \to \ldots$$

is exact.

(II) If $x \in M$ and if $x_P = 0$ for all maximal ideals P then $x = 0$.

Proof It $x \neq 0$ then $ann(x) \neq A$ (because $1.x \neq 0$), hence there exists a maximal ideal P containing $ann(x)$. Then $X_P \neq 0$.

THEOREM 1. If a system of linear equations

$$(*) \sum_{j=1}^{n} a_{ij} x_j = b_i,\ i = 1, \ldots; m \quad (a_{ij}, b_i \in A)$$

has a solution in A_P for every maximal ideal P of A, then it has a solution in A.

PROOF. Let $f : A^n \to A^m$ be the A-linear mapping given by $f(x_1, \ldots, x_n) =$

$(\Sigma a_{1j}x_j, \Sigma a_{2j}x_j, \ldots, \Sigma a_{mj}x_j)$, and let $\beta = (b_1, \ldots, b_m)$. Denote the cokernel of f by N. Thus $N = A^m/f(A^n)$. Let $\bar{\beta}$ be the image of β in N. Then (*) is solvable in A iff $\bar{\beta} = 0$. (*) is solvable in A_p iff $\bar{\beta}_p = 0$, because one can identify N_p with the cokernel of $f_p : A_p{}^n \to A_p^m$ induced by f. Thus the theorem follows from the remarks (II) above.

Determinantal Ideals Let $M = (u_{ij})$, $u_{ij} \in A$, be an $r \times s$ matrix. The rank of M is defined as usual, namely as the size of largest non-vanishing minors.

Let t be an integer between 1 and Min (r, s). The ideal generated by the $t \times t$ minors of M is denoted by $I_t(M)$. Consider the system of linear equations (*) and put

$$M = (a_{ij}), \quad M' = (M, \begin{matrix} \xi_1 \\ \vdots \\ \xi_m \end{matrix})$$

$$m \times n \qquad m \times (n+1)$$

If (*) has a solution in A then the last column of M' is a linear combination of the columns of M. Hence:

THEOREM 2.

If (*) is solvable is A, then

$$I_t(M) = I_t(M') \quad \text{for all } t.$$

Remark: In general this condition is not sufficient.

An integral domain A is called a *Dedekind domain* if (1) it is noetherian and (2) A_p is a discrete valuation ring for every non-zero prime ideal P. (A discrete valuation ring is a principal ideal domain which has a unique maximal ideal (π), so that the non-zero ideals are (π^n), $n = 1, 2, \ldots$.) The ring of algebraic integers in a number field (i.e. a finite extension field of Q) K is a typical example of a Dedekind domain.

THEOREM 3

If A is a Dedekind domain, then the system (*) of linear equations is solvable in A iff

(1) rank M = rank M', and

(2) $I_r(M) = I_r(M')$ where r = rank M.

Example

$$\begin{cases} 3x + 4y + 5z = 2 \\ x - 2y + z = 2 \end{cases} \qquad A = Z \qquad r = 2$$

$$I_r(M) = I_r(M') = 2Z.$$

Therefore it is solvable in Z.

Proof of Th. 3. By localization we may assume that A is a discrete valuation ring. Then by elementary transformations on the variables and on the equations we can bring (*) to the following form:

$$\pi^{e_i} x_i = b_i', \quad i = 1, \ldots, r; \qquad e_1 \leqslant e_2 \leqslant \ldots \leqslant e_r,$$

where π is a prime element of A. (This is the so-called elementary divisor theorem.) Then $I_r(M) = \pi^{e_1 + \ldots + e_r} A$, and $I_r(M) = I_r(M')$ implies $b_i' \in \pi^{e_i} A$ as one can immediately check.

When A = Z this theorem was found in 1856. Since the elementary divisor theorem is valid only in principal ideal domains, localization (i.e. Th. 1) is essential in the generalization to Dedekind domains. We also like to point out that if there is only one equation then Th. 3 is just a tautology. The value of Th. 3 is to reduce the solvability of a system to that of a single equation.

The Dedekind domains are, ring-theoretically, characterized as the one-dimensional, integrally closed noetherian domains. For more general rings (e.g. for a polynomial ring $k[x, y]$ over a field k, which is a two-dimensional integrally closed noetherian domain) no useful necessary and sufficient conditions seem to be known.

§ 2. Artin Approximation Theorems.

From now on, we will mean by a local ring a noetherian local ring. A local ring (A, m) has the m-adic topology, in which a fundamental system of neighbourhood of an element x of A is given by $\{ x + m^{\nu} \mid \nu = 1, 2, \ldots \}$. A complete local ring is a local ring in which every Cauchy sequence (in m-adic topology) converges. Every local ring has its completion. The ring of p-adic integers (invented by Hensel in the 19th century) is the completion of Z_{pz}. The completion of the convergent power series ring $C\{x_1, \ldots, x_n\}$ is the formal power series ring $C[\![x_1, \ldots, x_n]\!]$.

The classical lemma of Hensel is stated as follows:

Hensel's Lemma.

Let A be a complete local ring and let $k = A/m$ be its residue field. Let $f(x) = x^n + a_1 x^{n-1} + \ldots + a_n \in A[x]$ and let $\bar{f}(x) = x^n + \bar{a}_1 x^{n-1} + \ldots + \bar{a}_n \in k[x]$ be its image in $k[x]$. If $\bar{f}(x)$ has a simple root c in k, then $f(x)$ has a root $\alpha \in A$ such that $\bar{\alpha} = c$.

This is an algebraic analogy of the implicit function theorem in analysis [if $f(x, y)$ is C^∞ in a neighbourhood of (o, c) and $f(o, c) = 0$, $\frac{\partial f}{\partial y}(o,c) \neq 0$, then there exists a C^∞ function $y = y(x)$ such that $f(x, y(x)) = 0$ and $y(0) = c$] and is easily proved by successive approximation.

A local ring for which the conclusion of Hensel's Lemma holds is called a Henselian local ring. G. Azumaya and M. Nagata studied the properties of Henselian local rings. In particular, Nagata proved the existence of Henselization for every local ring. If A is the local ring of a polynomial ring $k[x_1, \ldots, x_n]$ (k = a field) at the maximal ideal $(x_1, \ldots, x_n)$, then its Henselization is the ring of algebraic power series, i.e. the set of those elements of the completion $\hat{A} = k[\![x_1, \ldots, x_n]\!]$ which are algebraic over A.

M. Artin and some other algebraists (mainly in eastern Europe) have shown that Henselian rings have very good properties. The convergent power series ring $k\{\underline{x}\} = k\{x_1, \ldots, x_n\}$ (k = C or R, say) is a Henselian local ring. M. Artin first published the following analytic theorem:

Theorem (inventiones Math. 5, 1968)

Let $f_i(x, y) \in k\{x_1, \ldots, x_n; y_1, \ldots, y_m\}$, $1 \leqslant i \leqslant r$.

Let $\hat{y}(x) = (\hat{y}_1(x), \ldots, \hat{y}_m(x))$, $\hat{y}_j \in k[\![\underline{x}]\!]$ $\hat{y}_j(0) = 0$, be a solution of $f(x, y) = 0$, and let $c > 0$ be an integer.
Then there exist $y(x) = (y_1(x), \ldots, y_m(x))$, $y_j(x) \in k\{\underline{x}\}$, such that

$$f(x, y(x)) = 0, \quad y_j \equiv \hat{y}_j \bmod \hat{m}^c,$$

where $\hat{m} = \Sigma x_i k[\![\underline{x}]\!]$

According to this theorem, to solve the system of analytic equations one has only to find a formal solution. Convergent solutions can be found without any additional effort.

Remark: The condition $\hat{y}_j(0)$ is superfluous if f_i's are polynomials.

Application. Let $A = k\{x_1, \ldots, x_n\}$ and $\hat{A} = k[\![x_1, \ldots, x_n]\!]$ (k = R or C), and let $\varphi(x) \in m_A$. If $\varphi(x)$ is irreducible in $\hat{A}$ then it is irreducible in A.

Proof. Consider the equation

$$(\sum_{i=1}^{n} x_i T_i)(\sum_{j=1}^{n} x_j U_j) = \varphi(x).$$

This is a polynomial equation in $T_1,\ldots,T_n, U_1,\ldots,U_n$, with coefficients in A. If it has a solution in $\hat{A}$ then it has a solution in A by Artin's theorem.

We now turn to the algebraic version of the theory. Let A be a local ring, m its maximal ideal and $\hat{A}$ its completion. Consider the following properties: (WAP) Let $f = (f_1,\ldots,f_m)$, $f_i \in A[Y] = A[Y_1,\ldots,Y_N]$. If $f = 0$ has a solution in $\hat{A}$, then it has a solution in A. (AP) f being as before, if $\hat{y} = (\hat{y}_1,\ldots,\hat{y}_N)$ is a solution of $f = 0$ in $\hat{A}$ and if $c \in N$ is given, then there exists a solution $y = (y_1,\ldots,y_N)$ in A such that $y_j \equiv \hat{y}_j$ mod. $\hat{m}^c$, where $\hat{m}$ is the maximal ideal of $\hat{A}$.

(SAP) For a given f as before, there exists a function $\nu : N \to N$ with the following property:

if $\bar{y} = (\bar{y}_1,\ldots,\bar{y}_N) \in A^N$ satisfies $f(\bar{y}) \equiv 0 \bmod m^{\nu(c)}$, then there is $y \in A^N$ such that $f(y) = 0$ *and* $y \equiv \bar{y} \bmod m^c$.

It is easy to see that (SAP) $\Rightarrow$ (AP) $\Leftrightarrow$ (WAP). actually all three properties are equivalent.

Greenberg (1967) proved that excellent Henselian discrete valuation rings have (SAP).

Artin (1969) proved that algebraic power series rings over a field have (SAP).

Pfister-Popescu (1975) proved that all complete local rings have (SAP). It follows from this that (SAP) and (AP) are equivalent. Later an entirely new proof was given to their theorem; the new proof is based on ultraproduct construction, a favorite tool of logicians.

Popescu (to appear) proved that excellent henselian local rings have (AP).

It is easy to see that a local ring with (AP) must be henselian. It has been conjectured that such a ring must also be excellent. In this direction, *Rotthaus* proved that if A and $A[\![x]\!]$ have (AP) then A must be excellent.

Application 1.

Let $A = k[\![x_1,\ldots,x_n]\!]$ be a formal power series ring over a field k, and let $\varphi(x) \in m_A$ be irreducible. Consider the equation

$$(*) \qquad (\sum_{i=1}^{n} x_i T_i)\,(\sum_{j=1}^{n} x_j U_j) = \varphi(x).$$

Since A has (SAP) by Pfister-Popescu, there is a function ν: IN $\to$ IN as in (SAP), for this equation. Put $r = \nu(1)$. Then (*) has no solution in A/m^r (otherwise (*) would have a solution in A, making $\varphi(x)$ reducible). But the image of (*) in $(A/m^r)[T, U]$ is the same if we replace $\varphi(x)$ by $\Psi(x)$ such that $\Psi \equiv \varphi \bmod m^r$. Therefore, all such $\Psi(x) \in A$ are irreducible. In short, all formal power series sufficiently close to φ are irreducible.

Application 2 M. Hochster used Artin's result to prove the existence of so-called 'big Cohen-Macaulay modules" for local rings which contain fields. We cannot explain the meaning of Hochster's result here, but it is considered as one of the most important achievements in Commutative Algebra in recent years. He gives a standard way of constructing of an infinitely generated module, and shows that the module thus constructed satisfies the requirement if certain systems of algebraic equations have no solution in A. Then he proves the unsolvability directly in the case of characteristic p. Then he reduces the case of characteristic zero to the case of characteristic p by means of Artin approximation theorem.