On two conjectures about systems of algebraic equations

Harald Hule, Josef Schicho

September 30, 1997

Abstract

We give counterexamples for two conjectures relating the number of solutions of a system of algebraic equations to its property of being maximal.

1 Introduction

The solution of algebraic equations is surely one of the central and most ancient problems of mathematics and we need not discuss its practical usefulness. Equations over natural, integer, rational, real or complex numbers have a history of many centuries. Recently, equations over a multitude of algebraic structures have been investigated for theoretical and practical reasons. So, it is interesting to study the general case of universal algebras as it has been done by Lausch and Nöbauer ([1]).

We consider a universal algebra A in a variety $\mathcal{V}$. A system of algebraic equations in $x_1, \ldots, x_n$ over A is a family $S = (p_i, q_i)_{i \in I}$ with polynomials p_i, q_i in $x_1, \ldots, x_n$ over A in $\mathcal{V}$, i.e. elements of the polynomial algebra $A(X, \mathcal{V})$ with $X = \{x_1, \ldots, x_n\}$, in the sense of [1]. A pair (p_i, q_i) is called an equation and frequently written as "$p_i = q_i$". Instead of $x_1, x_2, \ldots$, we often use $x, y, \ldots$ as indeterminates.

A solution of S is an n-tuple $(u_1, \ldots, u_n)$ such that $p_i(u_1, \ldots, u_n) = q_i(u_1, \ldots, u_n)$ for all $i \in I$. These $u_1, \ldots u_n$ may be elements of A, but in general we have to look for solutions in extensions of A, i.e. in algebras $B \geq A$ with $B \in \mathcal{V}$. We call a system solvable iff there exists a solution $(u_1, \ldots, u_n) \in B^n$ for some extension $B \geq A$.

Let Θ be the congruence of $A(X, \mathcal{V})$ generated by S, i.e. by the pairs (p_i, q_i). Then it is well-known and easy to prove that S is solvable iff Θ separates the elements of A. In this case, we can embed A into $A(X, \mathcal{V})/\Theta$ in an obvious way and get an extension $A(S)$ of A. Then $(\overline{x_1}, \ldots, \overline{x_n})$ is a solution of S in $A(S)^n$. For any solution $(u_1, \ldots, u_n)$, the algebra $A(u_1, \ldots, u_n)$ (generated by

$A \cup \{u_1, \ldots, u_n\})$ is a homomorphic image of $A(S)$. Of course, there may exist other solutions in $A(S)^n$, even infinitely many. According to [2] and [3], we call a solvable system "of finite type" iff the number of solutions in $A(S)^n$ is finite.

We also need the notion of maximal systems of equations. A solvable system S is called maximal iff the congruence Θ is maximal among the congruences of $A(X, \mathcal{V})$ separating A. This means that any additional equation joined to S gives either a system equivalent to S (which has exactly the same solutions) or makes the system contradictory, i.e. not solvable.

A typical example of a system of finite type is the system consisting of an equation $p(x) = 0$, where $p(x)$ is an irreducible polynomial in x over a field K, considered as an algebra in the variety of commutative rings with identity. Then the congruence Θ corresponds to the ideal of $K[x]$ generated by $p(x)$. The algebra $K(S)$ is isomorphic to $K[x]/\langle p(x)\rangle$. It is also a field. The number of solutions of S in $K(S)$ is less or equal to the degree of $p(x)$ (whence finite type). In this classical case, three conditions are fulfilled.

(i) The variety is semidegenerate in the sense of [1], i.e. an algebra with more than one element cannot have a subalgebra with one element.

(ii) The algebra A is simple.

(iii) The system S is maximal.

The question arises whether there is a correlation between these conditions and the finite type property. Hule and Pilz showed in [2] that none of the conditions is necessary and that neither (i) and (ii), nor (i) and (iii) are sufficient for the finite type property. The question whether (ii) and (iii) or all three conditions together are sufficient remained open.

In [3], it was also shown that in the variety of abelian groups every solvable system S with a unique solution in $A(S)^n$ is maximal. This suggests the question whether this is true in general.

We can now answer both questions negatively.

2 A system with infinitely many solutions

We give a counterexample to the following

Conjecture 1 *Let $\mathcal{V}$ a semidegenerate variety. Let A be a simple algebra in $\mathcal{V}$. Let S be a maximal solvable system of equations over A, with n indeterminates. Then S has only finitely many solutions in $A(S)^n$.*

Let $\mathcal{V}$ be the variety of rings with unity. We take $A := \mathbf{Q}(i)$ (the commutative field of Gaussian numbers), and S the system

$$x^2 + 1 = ix + xi = 0.$$

In $A(S)$, we have $a\overline{x} = \overline{x}a$ for all $a \in \mathbf{Q}$. This is obvious for $a \in \mathbf{Z}$. For $a \in \mathbf{Z}$, $b \in \mathbf{Z} - \{0\}$, we get

$$ab^{-1}\overline{x} = ab^{-1}\overline{x}bb^{-1} = ab^{-1}b\overline{x}b^{-1} = a\overline{x}b^{-1} = \overline{x}ab^{-1}.$$

Then the elements of $A(S)$ can uniquely be written in the normal form $a + bi + c\overline{x} + di\overline{x}$ with $a, b, c, d \in \mathbf{Q}$. So, $A(S)$ is isomorphic to the skew field of quaternions with rational components. Since $A(S)$ is simple, S is maximal.

If $a, b \in Z$ are such that $a^2 + b^2$ is a square, then

$$\frac{a + bi}{\sqrt{a^2 + b^2}}\overline{x} \in A(S)$$

is a solution of S. There are infinitely many such solutions, hence S is not of finite type.

3 A system with a unique solution

We give a counterexample to the following

Conjecture 2 *Let $\mathcal{V}$ be a variety. Let A be an algebra in $\mathcal{V}$. Let S be a solvable system of equations over A with n indeterminates that has only one solution in $A(S)^n$. Then A is maximal solvable.*

Let $\mathcal{V}$ be the variety of commutative rings with unity. We take $A := \mathbf{Q}$, and S the system

$$(x^3 - 2)(x^5 - 2) = 0.$$

S is not maximal solvable, since it is properly contained in the solvable system $x^3 - 2 = 0$ (or $x^5 - 2 = 0$). The extension $A(S)$ is isomorphic to

$$\mathbf{Q}[x]/((x^3 - 2)(x^5 - 2)) \cong \mathbf{Q}[x]/(x^3 - 2) \times \mathbf{Q}[x]/(x^5 - 2) =: k_1 \times k_2.$$

The second isomorphism is a consequence of the Chinese remainder theorem, since $x^3 - 2$ and $x^5 - 2$ are coprime in $\mathbf{Q}[x]$.

The number of solutions of S in $k_1 \times k_2$ is equal to the number of solutions of S in k_1 times the number of solutions of S in k_2. We show that S has only one solution in k_1, the other part is analoguous.

Let X be a solution of S in k_1. Since k_1 is a field, we have either $X^3 - 2 = 0$ or $X^5 - 2 = 0$. Since k_1 can be seen as a subfield of the reals, $X^3 - 2 = 0$ has only one solution in k_1 (namely x).

The other case $X^5 - 2 = 0$ is impossible. If it were, then we would have a ring homomorphism $k_2 \to k_1$, mapping $x \in k_2$ to the solution X in k_1. This must be a field extension, hence $[k_2 : \mathbf{Q}] = 5$ divides $[k_1 : \mathbf{Q}] = 3$, which is not the case.

References

[1] H. Lausch, W. Nöbauer: Algebra of polynomials. North Holland, 1973.

[2] H. Hule, G. Pilz: Algebraische Gleichungssysteme über universellen Algebren. Inst.ber. 306, Math. Inst. Univ. Linz, 1986.

[3] H. Hule, G. Pilz: Equations over abelian groups. Contr. Gen. Algebra 5, Proc. Salzburg, 1986.