Solving Equations in Rings

One stated purpose of algebra is to formulate and solve equations. An important theorem (which will be proved in a later course on Algebra) states that *any* consistent finite system of algebraic equations in finitely many variables can be solved using matrices. Broadly speaking, this is Hilbert's Nullstellensatz (Null means zero, stellen means place and satz means statement or theorem).

First of all let us see this in the context of 1 variable. We have aready seen examples that there are *more* solutions to equations in general rings than there are in integers. For example, we produced a number of idempotents in matrices and $\mathbb{Z}/6$; on the other hand:

Exercise: Note that the only idempotents in $\mathbb{Z}$ are 0 and 1.

Given an equation of the type:

$$X^n + a_{n-1}X^{n-1} + \cdots + a_0 = 0$$

we would like to solve it. To do so we introduce the "companion" matrix which is an $n \times n$ matrix:

$$A = \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ -a_0 & -a_1 & -a_2 & \dots & \end{pmatrix}$$

Exercise: Check that A satisfies the above equation.

To understand this exercise, we must explain what it means to multiply a matrix A over R by an element a of R. We define $a \cdot A$ to be the multiplication of A (on the left) by the matrix which consists of a on the diagonal and 0 everywhere else. In fact,

Exercise: Show that the map that sends an element a or R to the $p \times p$ matrix $f(a)$ which has a on the diagonal and 0 everywhere else gives a ring homomorphism $f : R \to M_p(R)$.

We can also solve equations in $\mathbb{Z}n$. For example,

Exercise: Check that $2 \cdot 2 + 1 = 0$ in the ring $\mathbb{Z}/5$.

Exercise: Check that $2 \cdot 2 \cdot 2 - 1 = 0$ in the ring $\mathbb{Z}/7$.

Note that the equations $X^2 + 1 = 0$ has no solution in integers and the only solution of $X^3 - 1 = 0$ in integers is $X = 1$.

Remarks

While the above "solutions" of the equations may feel like "cheating", these are actually quite useful! When someone asks you to solve an equation, you *must* ask them what they want to use the solution for. Only if you know how the solution is going to be used can you give a meaningful answer.

For example, if they want a solution in decimal numbers (or real numbers) it is important to know how accurate an answer is required, since, in general, there is "exact" answer. Moreover, you need to know how the accuracy will affect the use. For example, if it is the value of the left-hand side of the equation that needs to be small, then you need to measure accuracy differently!

In general, Hilbert's theorem underlines a principle in algebra: Any consistent system of equations has an "algebraic" (or "formal") solution. In fact, this can be seen as a "definition" of consistency! Thus, the first task in algebra is to *study* this algebraic solution (or solutions) which will lie in some ring R. The actual context in which you want to *use* the solution will be another ring S. The study of R will help to decide whether there is a ring homomorphism $R \to S$ or not and how it can be constructed. This will then be a complete solution in the context in which the solution is required.