On different kinds of multiplication

Bartosz Malman

August 22, 2014

I think most of us have some degree of confidence in our ability to multiply numbers. After all, we are taught how to perform integer multiplication already at a young age. Any curious person notices that this operation possesses a special property. Namely, if the numbers a and b are both different from zero, then their product, $a \cdot b$, is also different from zero. This is intuitively clear, at least when both a and b are natural numbers. The natural numbers are, of course, the numbers $1, 2, 3 \ldots$ and so on. After all, by buying three packs of *kanelbullar*, with six in each, we certainly will not end up hungry. It is probably also intuitively clear that the product of two non-zero rational (or real) numbers is non-zero. That the product of two non-zero complex numbers is again non-zero might be a little less intuitive, but our definitions make sure this also is the case.

It turns out that science, engineering and mathematics has a need of defining 'multiplication' of objects much different from numbers. A set of objects, or *elements*, which can be added and multiplied, is known in mathematics as a *ring*. Mathematicians define precisely what laws such a multiplication operation should obey. Curiously, they have decided that the non-vanishing of products of two non-zero elements should not be one of them! They also thought that it would be a little too restrictive to require that a multiplied by b should give the same result as b multiplied by a. Hence, in general, $a \cdot b \neq b \cdot a$ in a ring. The importance of the definition of a ring lies in its generality. Given two elements a and b of some ring, we can make sense of their sum $a + b$ and of their product $a \cdot b$, but we care not what a or b really are. They might be numbers, might be matrices, they might be anything. But whatever they are, we can add and multiply them. The study of multiplication in a special kind of rings, called *group rings*, was the subject of my thesis. Products can vanish in a group ring, and the order of factors matters.

Both phenomena described above are known to first-year linear algebra students who are familiar with matrices and their rules of addition and multiplication. It is possible for the product of two non-zero matrices to be the zero matrix, and also the order of multiplication of matrices matters. Many students will agree that the multiplication of matrices seemed a little peculiar at first. This multiplication, together with corresponding matrix addition, makes the set of square matrices of some fixed size into a ring.

It is often important to know if a ring contains non-zero elements which vanish upon multiplication with some other non-zero elements. Such elements are called *zero-divisors*.

This notion is *abstract*, but nevertheless it might have very real implications. As an example, we take systems of linear equations and indicate how the possibility to solve such a system relates to zero-divisors. Any student of science and engineering will know that systems of linear equations arise naturally in literally every branch of natural science or engineering. Fast and efficient methods of solving these systems are absolutely crucial. In fact, (systems of) linear equations are relatively easy to handle, while non-linear equations are so difficult that we rather just approximate them with linear ones, and solve the approximations instead.

Assume then that we have a system of linear equations, and that we have as many equations as we have unknown variables. Such a system we usually call *square*. A square system of linear equations can be modelled by one square matrix and one vector. A solution consists of any vector satisfying the equations of the system. Freshman students learn *matrix determinants*, and one of their applications is to be able to conclude easily if a square system of linear equations has a unique solution. We can also characterize this property using zero-divisors. It turns out that such a system of linear equations has a unique solution exactly when its matrix, viewed as an element of the ring of square matrices, is not a zero-divisor. If the matrix of the system is a zero-divisor, then a solution might or might not exist. If a solution exists, it is never unique. This can lead to trouble in different ways. In this sense, matrices that are zero-divisors are *bad* matrices. They do not behave nicely, and they model systems of linear equations that do not have unique solutions.

I mentioned above a special class of rings, the group rings. It would be a little too technical to explain here how a group ring differs from a general ring, so we have to content ourselves with the claim that from every possible ring one can construct many group rings. One very famous question, initially posed by the brilliant mathematician Irving Kaplansky, asks to classify the group rings in which multiplication resembles in a way our familiar multiplication of numbers. More precisely, he conjectured that a certain type of group rings were always free of zero-divisors. The problem is to rigorously prove his claim. I have spent some time investigating the current status of the problem as part of my work on my thesis. The result? I understand how unapproachable it is. The question is today almost 50 years old, and so far nobody has been able to confirm that Kaplansky was right, and nobody has been able to prove him wrong.

Much of work in contemporary mathematics, and indeed many other sciences, including computer science and physics, is abstract (and for a good reason, but that is a topic for another discussion). But very recently, a real-world application of group rings has been proposed, in form of the construction of a versatile cryptographic system [1]. To be able to understand how such a system might work, we will need to know what a *multiplicative identity element* and what a *unit* is. We are unfortunately (or fortunately?) back to abstraction.

A multiplicative identity is an element of the ring, which multiplied by any non-zero element a gives us back a. This element is often denoted by 1, because it behaves similarly to the number 1. Hence $1 \cdot a = a \cdot 1 = a$. An element u is a unit if there exists an element v such that $u \cdot v = v \cdot u = 1$. The element v is called the *inverse* of u. Far from every element of a group ring is a unit. If we look again at matrices which model square systems of linear equations, then any matrix which is a unit is a *good* matrix. A unit matrix models a system of linear equations which has a unique solution. As we will see below, units in group rings also let us encrypt messages.

Given a message to transmit, it is possible to construct a group ring in which the message appears (encoded) as an element. Let us assume that the element w of the group ring is our message. If the recipient of our message hands us a unit u, then the encryption of the message w is performed by multiplication by u. That is, the encrypted message is $u \cdot w$. As our recipient receives the encrypted message, he or she can now multiply the encrypted message by v, resulting in $v \cdot u \cdot w = (v \cdot u) \cdot w = 1 \cdot w = w$. This is the initial message, as a group ring element! The recipient can now translate the element w into the original message. Of course, all these computational steps are performed by a computer. The strength of the system lies in the fact that units are hard to find in group rings. A careful choice of a unit u makes it near impossible to find its inverse v using computers of today. The recipient of the messages can hand over the same unit u to several sources which wish to communicate, and be the only one to be able to decrypt the incoming messages. This is the principle of *public-key cryptography*, with the unit u being the public key.

Using special kinds of multiplication as encryption is not really a recent development. The ideas are almost 40 years old, and have indeed turned out to be very useful. The famous RSA cryptosystem based upon ring multiplication is today widely used in many applications, one of them being digital signatures. The group ring encryption described above is a slightly more sophisticated version of the RSA cryptosystem.

Number arithmetic has historically introduced the ability to count and to measure. The general multiplication discussed above certainly has not been developed with such direct applications in mind. But nevertheless we have seen how this new notion can be used to reason about equations arising in all branches of natural science, and we have seen how it can be used to construct cryptographic systems. Even though the study of structures as abstract as rings is often driven simply by curiosity, perhaps the unexpected applications can be used as one argument to motivate their study.

References

[1] B. Hurley and T. Hurley, *Group ring cryptography* International Journal of Pure and Applied Mathematics, 60(1): 6786 (2011).