Factorization and the A+XB[X] construction

Muhammad Zafrullah
Department of Mathematics
University of Iowa
Iowa City, IA

Preamble

By factorization of a nonzero nonunit of an integral domain D, we generally mean, expressing the element as a product of other, simpler, elements.

The “simpler” elements are often, irreducible elements or atoms, i.e. ones that cannot be further expressed as products of two or more non units.

We study factorization because factorization properties of nonzero nonunits of an integral domain often lead to nice conclusions about the properties of the integral domain.

I usually talk about factorization that is more to do with expressing nonzero elements x of an integral domain D as products $x = uv$ where u comes from one kind of elements and v comes from another kind of elements, involving comaximality of one type or another.

This time I would look into the usual, plain notion of dividing; keep on dividing and hope that the process would stop at some place.

Restrictions can also make life easy

When the algebraists decided to move away from the integers and invented more general systems they found out that the processes such as dividing into two simpler parts, may not make sense (as in finite groups) and if it does the process may not end as in nondiscrete valuation rings. It was a woman (Emmy Noether) who first thought of putting some restrictions on the discourse. She said she would only study rings whose ideals satisfy the ascending chain condition and with laborious work gave birth to Noetherian rings.

Now as, in an integral domain D, a divides b means $bD \subseteq aD.$ So continuing dividing by nonunits would give rise to an ascending chain of proper principal ideals which must stop in a Noetherian domain, and some of those Noetherian domains, such as $K[X],$ for K a field displayed a sort of unique factorization, just like the integers, bingo. So, a Noetherian domain is atomic, i.e., every nonzero nonunit can be expressed as a finite product of irreducible elements or atoms, just like in integers. Simply look at $xD \subsetneq a_1D \subsetneq a_2D \subsetneq \ldots \subsetneq a_mD \subsetneq \ldots$ by the Noetherian condition it will stop for some finite value of $m.$ Set such an $a_m = q_1$. This q_1 cannot be expressed as a product of two nonunits, for if it did the chain did not stop at $m.$ Repeat the above procedure with (x/q_1D) and continue and by the chain condition it would end at say $(q_2)D.$ Again repeat the dividing on $(x/q_1q_2)D.$ Continuing this way you will end up with a sequence $xD \subsetneq (x/q_1D) \subsetneq (x/q_1q_2)D \subsetneq \ldots \subsetneq (x/q_1q_2\ldots q_n)D$ ... Again by the Noetherian condition this must stop for some $n,$ at an atom and that will give you the atomic factorization. (When we are doing factorization of elements Ascending Chain Condition on Principal ideals (ACCP) is enough.)

But factorization in a Noetherian domain does not guarantee uniqueness and workers in algebraic number theory had, painfully, known before Noether that there were serpents in the paradise. There were some rings of algebraic integers that did not have unique factorization and they had to settle for unique factorizations of ideal numbers (ideals). Any ring of algebraic integers that is not a PID would serve as an example but easier examples became folklore to demonstrate the fact. One of those examples is: $Z[\sqrt{-5}]$.

In an atomic domain we can talk about the atomic factorization of an element x as $x = a_1 a_2 \ldots a_n$ where each of a_i is an atom. The number n can be called the length of the atomic factorization. A Unique Factorization Domain is an integral domain D such that (a) it is atomic, (b) every atomic factorization of a nonzero nonunit is of the same length, and (c) the same set of atoms appears in every atomic factorization of a fixed nonzero nonunit.

How does this relate to the A + XB[X] construction?

(By the way $A + XB[X] = \{f(X) \in B[X],$ $f(0) \in A\}$ and A is a subring of B obviously.)

I have spent most of my working life running away from Commutative Ring Theory, as there seemed to be no future in it. After I left Libya, I stayed in Britain essentially to do some research and squander, as my wife would say, the savings. While I was there, in London, I heard of a course on algebraic coding theory being offered at Imperial College. I thought it was algebra and near enough. During that course a question of "non-unique factorization" came up. Two things happened: (a) the guy gave a definition of an atom as: a nonzero nonunit such that if $a = xy$ then $a \mid x$ or $a \mid y$ and unthinkingly, I jumped and said, "That’s the definition of a prime!" and immediately realizing my mistake slumped into the chair. (b) He gave the (then?) standard example of $6 = 2 \times 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ of non-unique factorization and, again quite unthinkingly, I blurted out "Why don’t you use $Q+XR[X]$ as an example of an atomic domain that is not factorial? It is atomic because of the degree considerations and because the constants are all units, and $X \mid (\pi X)(X/\pi)$ while X does not divide either of $(\pi X),(X/\pi)$." (here Q and R are respectively rational and real numbers.) I was working on my only paper with Alain Bouvier, where we showed that the so-called "t-class group" of rings like $Q+XR[X]$ is zero. It turned out the example hit home with the professor, whose name I do not remember. Next time he came to the LMS meeting, which was usually held at the University College London, he mentioned that to Paul Cohn, who was writing another algebra book and lo and behold that example got in one of the exercises. (I came to know about it when I was in the US, after having coauthored some of the papers that among others mentioned the above example.)

Is that the only A $+$ XB$[$X$]$ example of non-unique factorization?

Nah there are plenty. When I was in Iowa City the first time, looking at my preoccupation with the $A+XB[X]$ construction and factorization, Dan Anderson and his brother David decided to give these domains and factorization a thorough look. We wrote three papers [Houston J. Math. 17(1)(1991), 109-129], [J. Pure Appl. Algebra 69(1990),1-19], [J. Algebra 152(1992), 78-93] in which various new types of factorization were introduced. But what takes the cake even today was a result by Barucci, Izelgue and Kabbaj [Lecture Notes in Pure and Applied Math., Dekker, 1997, pp. 69-78]. They showed that if, A is a field then for any domain B containing A as a subring, $A+XB[X]$ satisfies ACCP. The argument that I gave for $Q+XR[X]$ would simply take care of this too.

In the above mentioned three papers, we

touched on a number of topics. One of them was half factoriality. An integral domain D is a Half Factorial Domain (HFD) if it is atomic and every nonzero nonunit of D has a unique length of atomic factorizations. It turned out that $Q+XR[X]$ is a half factorial domain that is not factorial. Reason: Every nonzero element of this ring is of the form $rX^s(1+Xf(X))$ where the part within the brackets can be shown to be a product of primes and if $s=0$ then $r\in Q$ and if $s>0$ rX^s can be expressed exactly as a product of s atoms, in an infinite number of distinct ways.

Coykendall, Dumitrescu and myself showed in [Houston J. Math. 32(1)(2006) 33-46] that for A a field, $A+XB[X]$ is an HFD if and only if B is integrally closed. You can consult the above paper for the history of this result. I continue with a discussion of what happens if we assume that X is irreducible (or prime) in $A+XB[X]$.

Suppose that X is reducible in $R=A+XB[X]$. Then $X=f(X)g(X)$ where $f,g\in A+XB[X]$ and both are nonunits of $A+XB[X]$. Since

$X, f(X), g(X)$ are all polynomials of $B[X]$ we conclude that, as $X = f(X)g(X),$ either the degree of $f(X)$ is zero or the degree of $g(X)$ is zero. Say the degree of $f(X)$ is zero then $f(X) = a \in A\backslash\{0\},$ where a is a nonunit of A, and the degree of $g(X)$ is one. So $g(X) = bX + c.$ Setting $X = a(bX + c)$ and comparing the constants we have $c = 0.$ Thus $X = a(bX)$ where a and bX are both nonunits of $A + XB[X].$ Comparing coefficients in $X = a(bX)$ we have $ab = 1.$ Thus if X is reducible in R then there is a nonunit $a \in A$ such that $a^{-1} \in B.$ Conversely if there is a nonunit $a \in A$ such that $a^{-1} \in B$ then $X = a(a^{-1}X)$ and so X is reducible. Thus we conclude that X is reducible in $A + XB[X]$ if and only if there is a nonunit a in A such that $a^{-1} \in B.$ Equivalently X is irreducible in $A + XB[X]$ if and only if there is no nonzero nonunit in A with inverse in $B.$ So, given an extension $A \subseteq B$ of domains $U(B) \cap A = U(A)$ if and only if X is irreducible in $A + XB[X]$, where $U(D)$ denotes the set of units of the domain D.

Why am I devoting so much time to deciding when X is irreducible? Well, if $A+XB[X]$ is atomic then X will have to be an atom and the only available characterization of $A+XB[X]$ satisfying ACCP is: $R = A+XB[X]$ satisfies ACCP if and only if for each infinite sequence of nonzero nonunits $\{a_i\}_{n\geq 1}$ in $A,$

$\cap(a_1 a_2 \ldots a_n)B = 0,$ by Dumitrescu et al [Comm. Algebra 28(3), 2000, 1125-1139]. By deciding when X is an atom in $A+XB[X],$ I am asking: What more do we need to ensure that $A+XB[X]$ satisfies ACCP? (Besides A satisfying ACCP!)

On the other hand X being a prime in $A+XB[X]$ is a very big and decisive event.

Recall that a nonzero nonunit element p of a domain D is a prime if for $a, b \in D,\ p \mid ab$ implies that $p \mid a$ or $p \mid b.$ It is well known that X is a prime in $A[X]$. So if $A = B$ then X is a prime in $A+XB[X].$ Conversely let $b \in B\backslash A.$ Then $X \mid (bX)(bX)$ but as $b \notin A,\ X \nmid bX$ and so X fails to be a prime. Thus we conclude that X is a prime in $A+XB[X]$ if and only if $A = B.$ We know that in this case $A+XB[X] = A[X]$ satisfies ACCP if and only if

A satisfies ACCP.

Part of the above discussion is taken from an answer to a question sent to my MIT helpdesk at www.lohar.com

Tiberiu Dumitrescu came up with the following approach to the "prime question".

Recall that if M is an A-module then the A-idealization of M is the set $A \times M$ endowed with the usual component-wise addition and with multiplication defined by $(a_1, m_1)(a_2, m_2) = (a_1 a_2,\ a_1 m_2 + a_2 m_1)$. You can read about idealization in Anderson and Winder’s paper “Idealization of a module” [J. Commut. Algebra 1 (2009), no. 1, 3–56], where idealization of M by A is denoted by $A(+)M$. That, for an A-module M, $A(+)M$ is a ring is clear from the definitions of addition and multiplication. Note that for all $m \in M$, $(0, m)^2 = (0, 0)$. So, we have the following statement.

$(*)$ $A(+)M$ is an integral domain if and only if A is an integral domain and $M = 0$. (If $A(+)M$ is an integral domain then for $m \in M$, $(0, m)^2 = (0, 0)$ forces $(0, m) = (0, 0)$ and so makes $M = (0)$. This makes $A(+)M \cong A$ and so A must be an integral domain. The converse is clear.)

Now $R/XR = \{(a+bX)\operatorname{mod}(X) : a \in A,\ b \in B\}$. The equality $(a+bX)\operatorname{mod}(X) = (a_1+b_1X)\operatorname{mod}(X)$ forces $a - a_1 + (b-b_1)X \in (X)$ which forces $a = a_1$ and $b - b_1 \in A$. Thus R/XR can be identified with $A \times B/A$. Of course it is easy to check that B/A is an A-module. Next as $((a+bX)\operatorname{mod}(X))((a_1+b_1X)\operatorname{mod}(X)) = (aa_1 + (ab_1 + a_1b)X)\operatorname{mod}(X)$ and as the addition $\operatorname{mod}(X)$ is given by $((a+bX)\operatorname{mod}(X)) + ((a_1+b_1X)\operatorname{mod}(X)) = (a + a_1 + (b+b_1)X)\operatorname{mod}(X)$. It is now easy to see that R/XR is isomorphic to $A(+)B/A =$ the A-idealization of the A-module B/A. Now X is a prime in $R = A + XB[X]$ if and only if $R/XR \cong A(+)B/A$ is an integral domain, which by $(*)$ is possible if and only if $B/A = (0)$ which is possible if and only if $A = B$.

This raises several questions. Of them one that I dare put forward is: Can we use this "idealization approach" to decide when an

$A + XB[X]$ domain is an HFD?

Indeed it might be useful to study the structure of $A + XB[X]/f(X),$ albeit in some very special cases