JOINT ZOOM-WEBINAR

Algebra Seminar

Alfréd Rényi Institute of Mathematics, Budapest

and

Algebra and Logic Seminar

Institute of Mathematics and Informatics

Bulgarian Academy of Sciences, Sofia

I. Anniversary: 150 Years of idempotents
II. Idempotents of 2×2 matrix rings over rings of formal power series

Vesselin Drensky

November 23, 2020

This project was carried out in the framework
of the exchange program
between the Hungarian and Bulgarian Academies of Sciences:
Joint research project “Combinatorial Ring theory”.

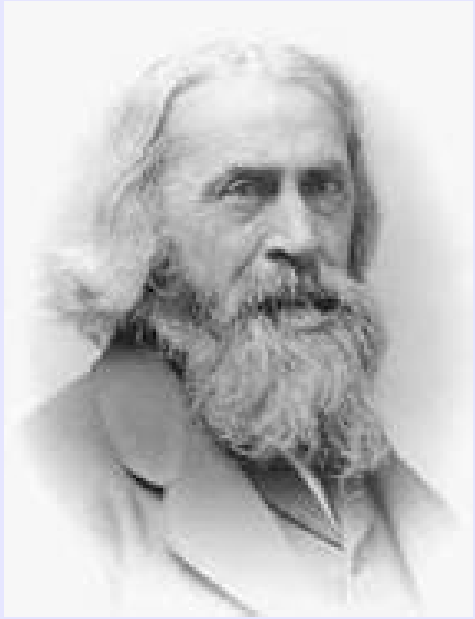
Partially supported by the Bulgarian National Science Fund
under Grant KP-06 N 32/1 of 07.12.2019
“Groups and Rings – Theory and Applications”.

I. Anniversary: 150 Years of idempotents

An element a in a ring A is called an idempotent if $a^2 = a$.
In 2020 we celebrate an anniversary of the idempotents – 150 years of their discovery. The idempotents were introduced in Ring Theory by Benjamin Peirce in 1870. Already 150 years their study is among the main topics in Ring Theory and its applications. For example the search in the database of Mathematical Reviews gives more than 2600 publications with the word "idempotents" in the title.

A couple of words for Benjamin Peirce

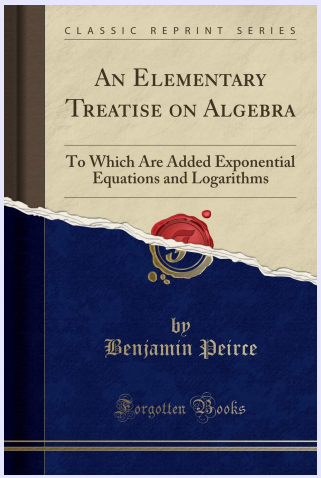
(Taken from https://mathshistory.st-andrews.ac.uk/Biographies/Peirce_Benjamin/)

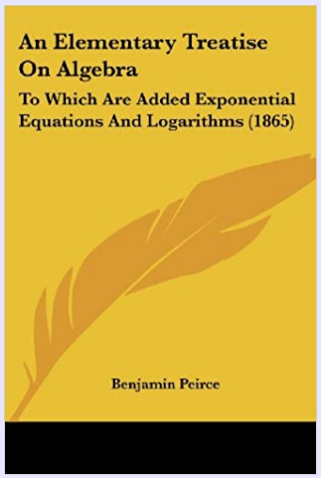


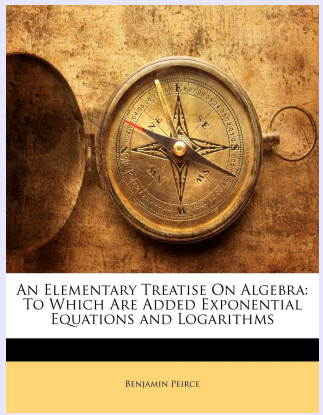
Benjamin Peirce
4 April 1809 – 6 October 1880

Benjamin Peirce was a remarkable person. He spent the whole of his career in Harvard, starting from 1831 until his death.

In the beginning of his career Peirce published a number of original and mathematically elegant textbooks which turned to be too difficult for the Amercian students. All of them were named *An Elementary Treatise: on Plane Trigonometry, on Spherical Trigonometry, on Sound, on Algebra: To which are added Exponential Equations and Logarithms, etc.*







Peirce made contributions on a wide range of mathematical topics – from celestial mechanics and geodesy in applied mathematics to linear associative algebra and number theory in pure mathematics. He helped determine the orbit of Neptune (discovered in 1846) and calculated the perturbations produced by Neptune on the orbit of Uranus and on the other planets.

Peirce introduced methods into the theory of errors applied to observations which would allow faulty observations to be discarded. There was an interesting consequence of this, namely that he was called as an expert witness in a court case which concerned the forging of the signature on a contested will.

Peirce was involved in a major way in the United States Coast Survey, as director of the longitude determinations and then as director of the institution, and overseeing the production of a map of the United States. He organised expeditions by the Survey to Sicily, Nagasaki, the Chatham Islands, and Alaska to observe astronomical events.

In 1863 Pierce was one of the founders of the National Academy of Sciences of the United States. He was also elected to the American Philosophical Society (1842), the Royal Astronomical Society (1850), and the Royal Society (1852).

The following text from the address of Peirce to the American Association for the Year 1853 as its President shows his strong believe in mathematics:
Mathematics is the great master-key, which unlocks every door of knowledge, and without which no discovery – no discovery which deserves the name, which is law and not isolated fact – has been or ever can be made.

Back to the history of idempotents

Peirce presented his results to the National Academy of Sciences in Washington in 1870 but they could not afford to print them.
By an initiative taken by Coast Survey staff, a lady without mathematical training but possessing a fine hand was found who could both read his ghastly script and write out the entire text 12 pages at a time on lithograph stones. As a result, in 1870 Peirce published his seminal book
B. Peirce, *Linear Associative Algebra*, Washington, 1870.
http://www.math.harvard.edu/history/peirce_algebra/index.html
The book was published lithographically at his own expense in 100 copies for distribution among his friends.

LINEAR ASSOCIATIVE

ALGEBRA

BY

BENJAMIN PEIRCE, LL. D.

Perkins Professor of Math. and Astron. at Harvard University

and Superintendent of the United States Coast Survey.

Read before the National Academy of Sciences.

WASHINGTON CITY.

1870

To my friends.

This work has been the pleasantest mathematical effort of my life. In no other have I seemed to myself to have received so full a reward for my mental labor in the novelty and breadth of the results. I presume that to the uninitiated the formulae will appear cold and cheerless. But let it be remembered that, like other mathematical formulae, they find their origin in the divine source of all geometry. Whether I shall have the satisfaction of taking part in their exposition, or whether that will remain for some more profound expositor, will be seen in the future.

B. P.

To my friends

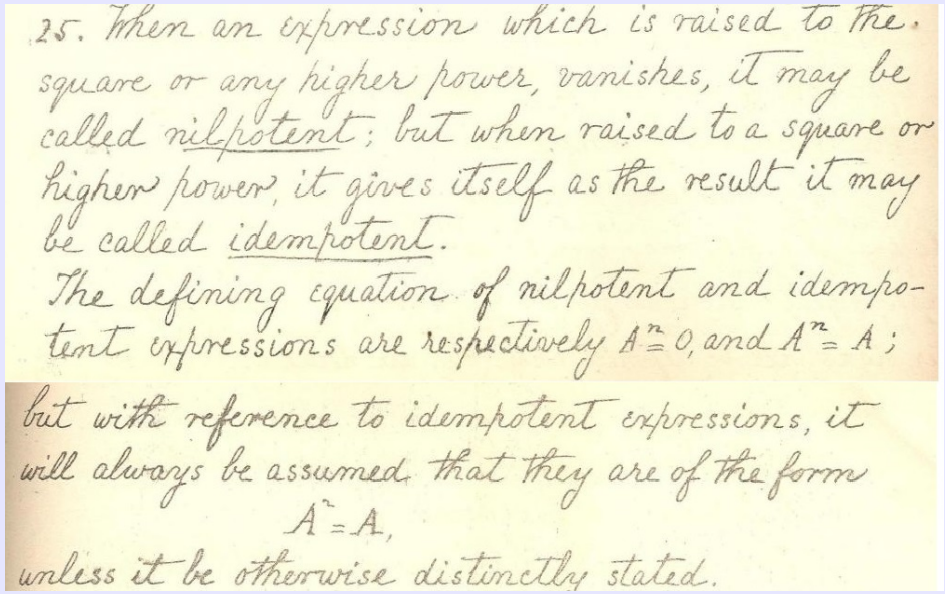
This work has been the pleasantest mathematical effort of my life. In no other have I seemed to myself to have received to full a reward for my mental labor in the novelty and breadth of the results. I presume that to the uninitiated the formulae will appear cold and cheerless. But let it be remembered that, like other mathematical formulae, they find their origin in the divine source of all geometry. Whether I shall have the satisfaction of taking part in their exposition, or whether that will remain for some more profound expositor, will be seen in the future.

B.P.

With the agreement of Sylvester, editor of American Journal of Mathematics, the book was reprinted posthumously in 1881 with addenda of his son C.S. Peirce:
B. Peirce, *Linear Associative Algebra*, Reprinted: Am. J. Math. **4** (1881), 99-215, addenda: 215-229 (pp. 225-229 by C.S. Peirce).
It starts with the headnote
"This publication will, it is believed, supply a want which has been long and widely felt, and bring within the reach of the general mathematical public a work which may almost be entitled to take rank as the *Principia* of the philosophical study of the laws of algebraical operation."

Benjamin Peirce deserves recognition, not only as a founding father of American mathematics, but also as a founding father of modern abstract algebra.
(Helena M. Pycior, Benjamin Peirce's Linear Associative Algebra, Isis **70** (254) (1979), 537-551.)

In his book Peirce invented the terms of *idempotent* and *nilpotent elements* and used them to establish the foundations of a general theory of linear associative algebra. In particular, he presented multiplication tables for over 150 new algebras.



25. When an expression which is raised to the square or any higher power, vanishes, it may be called nilpotent; but when raised to a square or higher power, it gives itself as the result it may be called idempotent.

The defining equation of nilpotent and idempotent expressions are respectively $A^n = 0$, and $A^n = A$;

but with reference to idempotent expressions, it will always be assumed that they are of the form

$$A^\infty = A,$$

unless it be otherwise distinctly stated.

25. When an expression raised to the square or any higher power vanishes, it may be called *nilpotent*; but when, raised to a square or higher power, it gives itself as the result, it may be called *idempotent*.
The defining equation of nilpotent and idempotent expressions are respectively $A^n = 0$, and $A^n = A$; but with reference to idempotent expressions, it will always be assumed that they are of the form

$$A^2 = A,$$

unless it be otherwise distinctly stated.

Origin from classical Latin

Idempotence literally means "(the quality of having) the same power", from idem + potence (same + power).
Nilpotent: from nil (not any) + potent (having power) with literal meaning "having zero power".

Existence of idempotent and nilpotent elements

40. In every linear associative algebra, there is at least one idempotent or one nilpotent expression.

Take any combination of letters at will and denote it by A. The square is generally independent of A, and its cube may also be independent of A and A^2. But there cannot be more powers of A, which are independent of A and of each other, than there are letters of the alphabet; so that there must be some least power of A, which is dependent upon the inferior powers. The mutual dependence of the powers of A, may be expressed in the form of an equation, of which the first member is an algebraic sum, such as

$$\Sigma_m (a_m A^m) = 0.$$

all the terms of this equation, which involve the square and higher powers of A may be combined and expressed as BA, so that B is itself an algebraic sum of powers of A, and the equation might be written

$$BA + a_1 A = (B + a_1) A = 0.$$

It is easy to deduce from this equation, successively,

$$(B + a_1) A^m = 0$$

$$(B + a_1) B = 0$$

$$\left(-\frac{B}{a_1}\right)^2 = -\frac{B}{a_1}$$

so that $-\frac{B}{a_1}$ is an idempotent expression. But if a_1 vanishes, this expression becomes infinite, and instead of it, we have the equation

$$B^2 = 0$$

so that B is a nilpotent expression.

40. *In every linear associative algebra, there is at least one idempotent or one nilpotent expression.*

Take any combination of letters at will and denote it by A. Its square is generally independent of A, and its cube may also be independent of A and A^2. But the number of powers of A that are independent of A and of each other, cannot exceed the number of letters of the alphabet; so that there must be some least power of A which is dependent upon the inferior powers. The mutual dependence of the powers of A may be expressed in the form of an equation of which the first member is an algebraic sum, such as

$$\Sigma_m(a_m A^m) = 0.$$

All the terms of this equation that involve the square and higher powers of A may be combined and expressed as BA, so that B is itself an algebraic sum of powers of A, and the equation may be written

$$BA + a_1 A = (B + a_1)A = 0.$$

It is easy to deduce from this equation successively

$$\begin{aligned} (B + a_1)\, A^m &= 0 \\ (B + a_1)\, B &= 0 \\ \left(-\frac{B}{a_1}\right)^2 &= -\frac{B}{a_1} \end{aligned}$$

so that $-\frac{B}{a_1}$ is an idempotent expression. But if a_1 vanishes, this expression becomes infinite, and instead of it we have the equation

$$B^2 = 0$$

so that B is a nilpotent expression.

Translation in modern language

In every (nonzero) finite dimensional associative algebra, there is at least one nonzero idempotent or one nonzero nilpotent element.

Proof. Let A be a finite dimensional associative algebra and let $a \neq 0$ be an element of A. Since the algebra is finite dimensional, there is an n such that the elements $a, a^2, \ldots, a^n$ are linearly dependent. Let $n \geq 2$ be the minimal integer with the property

$$\sum_{m=1}^{n} \alpha_m a^m = 0$$

for some elements $\alpha_1, \alpha_2, \ldots, \alpha_n$ in the base field ($\alpha_n \neq 0$). Hence for

$$b = \sum_{m=2}^{n} \alpha_m a^{m-1} \text{ we have } (b + \alpha_1)a = 0 \text{ and } b \neq 0.$$

From the equation $(b+\alpha_1)a=0$ it is easy to deduce that

$$(b+\alpha_1)a^m=0, \quad (b+\alpha_1)b=0.$$

If $\alpha_1 \neq 0$, then

$$\left(-\frac{b}{\alpha_1}\right)^2=-\frac{b}{\alpha_1}$$

and $-\dfrac{b}{\alpha_1}$ is an idempotent element. If $\alpha_1=0$, then

$$b^2=0$$

and b is a nilpotent element.

Peirce decomposition

41. When there is an idempotent expression in a linear associative algebra; it can be assumed as one of the independent units, and represented by one of the letters of the alphabet; and it may be called the basis.

The remaining units can be so selected as to be separable into four distinct groups.

With reference to the basis, the units of the first group are idemfactors; those of the second group are idemfaciend and nilfacient; those of the third group are idemfacient and nilfaciend; and those of the fourth group are nilfactors.

First. The possibility of the selection of all the remaining units as idemfaciend or nilfaciend is easily established. For if i is the idempotent base its definition gives

$$i^2 = i .$$

The product by the basis of another expression such as A, may be represented by B, so that

$$i A = B ,$$

which gives

$$i B = i^2 A = i A = B$$

$$i (A - B) = i A - i B = B - B = 0 .$$

whence it appears that B is idemfaciend, and $A - B$ is nilfaciend. In other words A is divided into two parts of which one is idemfaciend and the other is nilfaciend; but, either of these parts may be wanting so as to leave A wholly idemfaciend or wholly nilfaciend.

Secondly. The still farther subdivision of these portions into idemfacient and nilfacient is easily shown to be possible by this same method, with the mere reversal of the relative position of the factors. Hence are obtained the required four groups.

The basis itself may be regarded as belonging to the first group.

41. When there is *an idempotent expression* in a linear associative algebra, it can be assumed as one of the independent units, and be represented by *one of the letters of the alphabet;* and it may be called *the basis.*

The remaining units can be so selected as to be separable into four distinct groups.

With reference to the basis, the units of the first group are idemfactors; those of the second group are idemfaciend and nilfacient; those of the third group are idemfacient and nilfaciend; and those of the fourth group are nilfactors.

First. The possibility of the selection of all the remaining units as idemfaciend or nilfaciend is easily established. For if i is the idempotent base, its definition gives

$$i^2 = i\,.$$

The product by the basis of another expression such as A may be represented by B, so that

$$iA = B\,,$$

which gives

$$iB = i^2A = iA = B$$
$$i(A - B) = iA - iB = B - B = 0\,,$$

whence it appears that B is idemfaciend and $A - B$ is nilfaciend. In other words, A is divided into two parts, of which one is idemfaciend and the other is nilfaciend; but either of these parts may be wanting, so as to leave A wholly idemfaciend or wholly nilfaciend.

Secondly. The still farther subdivision of these portions into idemfacient and nilfacient is easily shown to be possible by this same method, with the mere reversal of the relative position of the factors. Hence are obtained the required four groups.

The basis itself may be regarded as belonging to the first group.

Translation

Every associative ring A with an idempotent i has the decomposition as a direct sum

$$A = iAi \oplus iA(1-i) \oplus (1-i)Ai \oplus (1-i)A(1-i).$$

(If the ring is not unitary, then $(1-i)a$ means $a - ia$.)
Proof. For $a \in A$ we have $a = ia + (a - ia) \in iA + (1-i)A$. If $b \in iA \cap (1-i)A$, then $b = ia_1 = (1-i)a_2$,

$$ib = i(ia_1) = i^2 a_1 = ia_1 = b, \quad ib = i(1-i)a_2 = (i - i^2)a_2 = 0.$$

Hence $b = 0$ and $A = iA \oplus (1-i)A$. Similarly for multiplication from the right.

II. Idempotents of 2×2 matrix rings over rings of formal power series

(Following V. Drensky, Idempotents of 2×2 matrix rings over rings of formal power series, arXiv:2006.15070v1 [math.RA])

It is well known that the idempotents of the $d \times d$ matrix algebra $M_d(F)$ over a field F coincide with the diagonalizable matrices with eigenvalues equal to 0 and 1.

In 1946 Foster described the commutative rings A with the property that the idempotents in $M_d(A)$ are diagonalizable for all d.
A.L. Foster, Maximal idempotent sets in a ring with unit, Duke Math. J. **13** (1946), 247-258

In 1966 Steger showed that important classes of rings have this property. Among them are polynomial rings in one variable over a principal ideal ring (also with zero divisors) and polynomial rings in two variables over a π-regular ring with finitely many idempotents. (The ring A is π-regular if for any $a \in A$ there exists an n such that $a^n \in a^n A a^n$.)
A. Steger, Diagonability of idempotent matrices, Pac. J. Math. **19** (1966), 535-542.

The results of Foster and Steger were generalized also for matrices over noncommutative rings.
G. Song, X. Guo, Diagonability of idempotent matrices over noncommutative rings, Linear Algebra Appl. **297** (1999), Nos 1-3, 1-7.

Gómez-Torrecillas, Kutas, Lobillo and Navarro presented an algorithm for computing a primitive idempotent of a central simple algebra over the field $\mathbb{F}_q(x)$ of rational functions over the finite field $\mathbb{F}_q$ with applications to coding theory.
J. Gómez-Torrecillas, P. Kutas, F.J. Lobillo, G. Navarro, Primitive idempotents in central simple algebras over $\mathbb{F}_q(t)$ with an application to coding theory, arXiv:2006.12116v1 [math.RA].

In 1967 J.A. Erdos proved that every singular matrix over a field is a product of idempotent matrices.
J.A. Erdos, On products of idempotent matrices, Glasg. Math. J. **8** (1967), 118-122.

See also the recent preprint of Nguyen and the references there for further developments in this direction.
D.Q.N. Nguyen, Effectively bounded idempotent generation of certain 2×2 singular matrices by idempotent matrices over real quadratic number rings, arXiv:2006.00733v1 [math.NT].

We give also references to two papers by Ánh, Birkenmeier and van Wyk:
P.N. Ánh, G.F. Birkenmeier, L. van Wyk, Idempotents and structures of rings, Linear Multilinear Algebra **64** (2016), No. 10, 2002-2029.
P.N. Ánh, G.F. Birkenmeier, L. van Wyk, Peirce decompositions, idempotents and rings, J. Algebra **564** (2020), 247-275.
In the first one the authors mimic the behavior of idempotents in matrix rings in a more general setup. The second paper considers different aspects of the study of idempotents in the classical spirit.

The following three papers which are related to the present talk:
For relations between the idempotents of A, $A[X]$ and $A[[X]]$ where X is a finite set of variables:
G.F. Birkenmeier, J.Y. Kim, J.K. Park, On polynomial extensions of principally quasi-Baer rings, Kyungpook Math. J. **40** (2000), No. 2, 247-253.
and
P. Kanwar, A. Leroy, J. Matczuk, Idempotents in ring extensions, J Algebra **389** (2013), 128-136.
For the properties of the idempotents in $\mathbb{Z}_n$:
K. Isham, L. Monroe, Arithmetic of idempotents in $\mathbb{Z}/m\mathbb{Z}$, arXiv:2005.05248v1 [math.RA].

Problem

Describe explicitly the idempotents of the matrix rings $M_d(A)$ and $M_d(A[x])$, respectively, over a commutative ring A and over the polynomial ring $A[x]$ if the idempotents of A are known.

Partial results for 2×2 matrix ring $M_2(\mathbb{Z}_n[x])$ for positive integers n with a small number of prime factors.

- Desctiption of the idempotents of $M_2(\mathbb{Z}_p[x])$, $M_2(\mathbb{Z}_{2p}[x])$ (p odd) and $M_2(\mathbb{Z}_{3p}[x])$ (for p prime, $p > 3$):
  P. Kanwar, M. Khatkar, R.K. Sharma, Idempotents and units of matrix rings over polynomial rings, Int. Electron. J. Algebra **22** (2017), 147-169.
- Desctiption of the idempotents in $M_2(\mathbb{Z}_{pq}[x])$ and $M_2(\mathbb{Z}_{p^2}[x])$, where p and q are any primes:
  J.M.P. Balmaceda, J.P. Datu, Idempotents in certain matrix rings over polynomial rings, Int. Electron. J. Algebra **27** (2020), 1-12.
- Description of the idempotents in $M_2(\mathbb{Z}_{pqr}[x])$ for three pairwise different primes greater than 3:
  G. Mittal, Non-trivial idempotents of the matrix rings over polynomial ring $\mathbb{Z}_{pqr}[x]$, Serdica Math. J. **46** (2020), No. 1, 89-100.

The main step in the three papers in the previous slide is the description of the idempotents in $M_2(A[x])$ where A is a commutative ring without non-trivial (i.e. different from 0 and 1) idempotents. Since this holds for $A = \mathbb{Z}_n$ for $n = p, p^2$ for p prime, the authors apply the Chinese remainder theorem and the Euler-Fermat theorem to handle the cases $n = p, 2p, 3p, p^2, pq, pqr$ for p, q, r prime.

Question of Mittal

Find the idempotents in $M_2(\mathbb{Z}_n[x])$ for any square-free integer $n > 1$.

Our main result

We simplify the ideas in the three papers cited two slide ago and give an explicit presentation of the idempotents of $M_2(A[[X]])$ where A is a direct sum of a finite number of commutative rings without non-trivial idempotents and $A[[X]]$ is the ring of formal power series in an arbitrary (also infinite) set of commuting variables.

Consequence

We describe the idempotents of $M_2(\mathbb{Z}_n[[X]])$ when n is an arbitrary positive integer greater than 1.

Our proofs are very transparent and use well known elementary arguments only. They are based on the Cayley-Hamilton theorem (for 2×2 matrices only), the Chinese remainder theorem and the Euler-Fermat theorem.

We assume that X is an arbitrary set of commuting variables and for a commutative ring A we consider the ring $A[[X]]$ of formal power series in X.
First we present elementary straightforward proofs of some well known facts on idempotents.

Lemma

(Partial case of a result of Birkenmeier, Kim, Park and Kanwar, Leroy, Matczuk)
Let A be a commutative ring without non-trivial idempotents. Then the ring $A[[X]]$ also has only trivial idempotents.

Proof. Let $a(X) = a_0 + a_1 + a_2 + \cdots \in A[[X]]$ be an idempotent, where a_i is the homogeneous component of degree i of $a(X)$. Let $a(X) \notin A$ and $a_1 = \cdots = a_{k-1} = 0$, $a_k \neq 0$. Since $a^2(X) = a(X)$, comparing the homogeneous components of $a(X)$ and $a^2(X)$ we obtain that $a_0^2 = a_0$ in A and $2a_0a_k = a_k$. Since A has trivial idempotents only, we have that either $a_0 = 1$ or $a_0 = 0$. Both cases are impossible: If $a_0 = 1$, then $2a_k = a_k$ and $a_k = 0$; if $a_0 = 0$, then again $a_k = 0$ which is a contradiction. Therefore the idempotent $a(X)$ belongs to A and hence is trivial.

Proposition

(Partial case of a result of Kanwar, Khatkar, Sharma)
Let A be a commutative ring without non-trivial idempotents. Then all idempotents in $M_2(A)$ are

$$a = \begin{pmatrix} \alpha & \beta \\ \gamma & 1-\alpha \end{pmatrix}, I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, 0_2 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix},$$

where $\alpha, \beta, \gamma \in A$ and $\alpha(1-\alpha) = \beta\gamma$.

Proof. Let

$$a = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in M_2(A), \quad \alpha, \beta, \gamma, \delta \in A,$$

be an idempotent. By the Cayley-Hamilton theorem we have

$$a^2 - \mathrm{tr}(a)a + \det(a)I_2 = 0_2.$$

Subtracting the equality $a^2 - a = 0_2$ we obtain that

$$(\mathrm{tr}(a) - 1)a = \det(a)I_2.$$

The determinant $\det(a)$ of a is an idempotent of A because the equality $a^2 = a$ implies $\det(a) = \det(a^2) = \det^2(a)$. Hence $\det(a) = 1$ or $\det(a) = 0$.

First, let $\det(a) = 1$. Comparing the entries of the matrices in the equality $(\mathrm{tr}(a) - 1)a = 0_2$ we obtain that

$$(\mathrm{tr}(a) - 1)\alpha = (\mathrm{tr}(a) - 1)\delta = 1, (\mathrm{tr}(a) - 1)\beta = (\mathrm{tr}(a) - 1)\gamma = 0.$$

Hence $(\mathrm{tr}(a) - 1)$ is invertible in A. This implies that $\beta = \gamma = 0$ and $\alpha = \delta \neq 0$. Hence $\alpha I_2 = a = a^2 = \alpha^2 I_2$ and α is an idempotent. Therefore $\alpha = 1$ and $a = I_2$.

Now, let $\det(a) = 0$. Hence $(\mathrm{tr}(a) - 1)a = 0_2$ and

$$(\mathrm{tr}(a) - 1)\alpha = (\mathrm{tr}(a) - 1)\delta, (\alpha + \delta - 1)\alpha = (\alpha + \delta - 1)\delta = 0,$$

$$(-(\alpha+\delta-1))^2 = (\alpha+\delta-1)\alpha+(\alpha+\delta-1)\delta-(\alpha+\delta-1) = -(\alpha+\delta-1).$$

We obtain that $-(\alpha + \delta - 1)$ is an idempotent and is equal to 1 or 0. The former case implies that $-a = 0_2$ and $a = 0_2$. In the latter case $\delta = 1 - \alpha$ and a has the desired form (**??**). Since $\det(a) = \alpha\delta - \beta\gamma = 0$ we obtain the restriction $\alpha(1 - \alpha) = \beta\gamma$. A direct verification shows that all matrices of this form are idempotents.

Corollary

Let $A_1, \ldots, A_s$ be commutative rings without non-trivial idempotents and $A = A_1 \oplus \cdots \oplus A_s$ be their direct sum. Then all idempotents $a(X) \in M_2(A[[X]])$ in the 2×2 matrix ring with entries from $A[[X]]$ are obtained by the following procedure. We split the set of indices $\{1, \ldots, s\}$ in three parts

$$P = \{p_1, \ldots, p_k\}, Q = \{q_1, \ldots, q_l\}, R = \{r_1, \ldots, r_m\}$$

and present A in the form $A = A_P \oplus A_Q \oplus A_R$, where

$$A_P = \bigoplus_{p \in P} A_p, A_Q = \bigoplus_{q \in Q} A_q, A_R = \bigoplus_{r \in R} A_r.$$

We choose power series $\alpha(X), \beta(X), \gamma(X) \in A_P[[X]]$ such that $\alpha(X)(1-\alpha(X)) = \beta(X)\gamma(X)$. Then $a(X) = (a_P(X), I_2, 0_2)$, where $I_2 \in M_2(A_Q[[X]])$, $0_2 \in M_2(A_R[[X]])$ and

$$a_P(X) = \begin{pmatrix} \alpha(X) & \beta(X) \\ \gamma(X) & 1-\alpha(X) \end{pmatrix} \in M_2(A_P[[X]]).$$

Proof. Since each A_i, $i = 1, \ldots, s$, does not have non-trivial idempotents, by the lemma the same holds for the rings of power series $A_i[[X]]$. Applying the proposition we obtain that the idempotents in $M_2(A_i[[X]])$ are of the form

$$a_i(X) = \begin{pmatrix} \alpha_i(X) & \beta_i(X) \\ \gamma_i(X) & 1 - \alpha_i(X) \end{pmatrix}, \quad \alpha_i(X)(1-\alpha_i(X)) = \beta_i(X)\gamma_i(X),$$

where $\alpha_i(X), \beta_i(X), \gamma_i(X) \in A_i[[X]]$, or $a_i(X) = I_2$, or $a_i(X) = 0_2$. We present the set $\{1, \ldots, s\}$ as a disjoint union of three subsets P, Q and R, where $p \in P$ if $a_p(X)$ is of the form

$$a_i(X) = \begin{pmatrix} \alpha_i(X) & \beta_i(X) \\ \gamma_i(X) & 1 - \alpha_i(X) \end{pmatrix}, \quad \alpha_i(X)(1-\alpha_i(X)) = \beta_i(X)\gamma_i(X),$$

$q \in Q$ if $a_q(X) = I_2^{(q)}$ (the identity matrix in $M_2(A_q[[X]])$) and $r \in R$ if $a_r(t) = 0_2^{(r)}$ (the zero matrix in $M_2(A_r[[X]])$).

Let

$$a(X) = (a_{p_1}(X), \ldots, a_{p_k}(X)) \in A_{p_1}[[X]] \oplus \cdots \oplus A_{p_k}[[X]].$$

Since $A_P[[X]] = A_{p_1}[[X]] \oplus \cdots \oplus A_{p_k}[[X]]$, we obtain that $a(X)$ has the form

$$a_P(X) = \begin{pmatrix} \alpha(X) & \beta(X) \\ \gamma(X) & 1 - \alpha(X) \end{pmatrix} \in M_2(A_P[[X]])$$

and

$$\begin{aligned} \alpha(X) &= (\alpha_{p_1}(X), \ldots, \alpha_{p_k}(X)), \\ \beta(X) &= (\beta_{p_1}(X), \ldots, \beta_{p_k}(X)), \\ \gamma(X) &= (\gamma_{p_1}(X), \ldots, \gamma_{p_k}(X)) \end{aligned}$$

satisfy the relation $\alpha(X)(1 - \alpha(X)) = \beta(X)\gamma(X)$ because the coordinate power series $\alpha_p(X), \beta_p(X), \gamma_p(X)$ satisfy $\alpha_p(X)(1 - \alpha_p(X)) = \beta_p(X)\gamma_p(X)$ for all $p = p_1, \ldots, p_k$.

Obviously $(I_2^{(q_1)}, \ldots, I_2^{(q_l)})$ equals the identity matrix in $M_2(A_Q[[X]])$ and $(0_2^{(r_1)}, \ldots, 0_2^{(r_l)})$ is the zero matrix in $M_2(A_R[[X]])$ which completes the proof.

We shall apply the latter corollary for $A = \mathbb{Z}_n$, $n > 1$. We need the following well known fact.

Lemma

Let p be a prime and $d > 0$. Then all the idempotents of the ring $\mathbb{Z}_{p^d}$ are trivial.

Proof. Let $\alpha \in \mathbb{Z}$ be such that its image $\overline{\alpha}$ in $\mathbb{Z}_{p^d}$ is an idempotent. Hence $\alpha^2 - \alpha \equiv 0 \pmod{p^d}$ and p^d divides $\alpha(\alpha - 1)$. Since α and $\alpha - 1$ are coprime, we have that either p^d divides α and $\overline{\alpha} = 0$ in $\mathbb{Z}_{p^d}$, or p^d divides $\alpha - 1$ and $\overline{\alpha} = 1$ in $\mathbb{Z}_{p^d}$.

The following theorem was the main motivation to start the present project.

Main theorem

Let $n > 1$ be a positive integer. Then all idempotents $a(X)$ in $M_2(\mathbb{Z}_n[[X]])$ are obtained in the following way. We present n as a product $n = PQR$ of three pairwise coprime positive integers P, Q, R. If $P > 1$ we choose three power series $\alpha(X), \beta(X), \gamma(X) \in \mathbb{Z}[[X]]$ such that $\alpha(X)(1 - \alpha(X)) \equiv \beta(X)\gamma(X) \pmod{P}$. Then modulo n

$$a(X) \equiv \begin{pmatrix} \overline{\alpha}(X) & \overline{\beta}(X) \\ \overline{\gamma}(X) & 1 - \overline{\alpha}(X) \end{pmatrix},$$

where:

(i) If $P, Q, R > 1$, then

$$\overline{\alpha}(X) \equiv (\alpha(X) + (1 - \alpha(X))P^{\varphi(Q)})(1 - (PQ)^{\varphi(R)}),$$

$$\overline{\beta}(X) \equiv \beta(X)(1 - P^{\varphi(Q)\varphi(R)}), \overline{\gamma}(X) \equiv \gamma(X)(1 - P^{\varphi(Q)\varphi(R)});$$

(ii) If $P, Q > 1$, $R = 1$, then

$$\overline{\alpha}(X) \equiv \alpha(X) + (1 - \alpha(X))P^{\varphi(Q)}, \overline{\beta}(X) \equiv \beta(X)(1 - P^{\varphi(Q)}),$$

$$\overline{\gamma}(X) \equiv \gamma(X)(1 - P^{\varphi(Q)});$$

(iii) If $P, R > 1$, $Q = 1$, then

$$\overline{\alpha}(X) \equiv \alpha(X)(1 - P^{\varphi(R)}), \overline{\beta}(X) \equiv \beta(X)(1 - P^{\varphi(R)}),$$

$$\overline{\gamma}(X) \equiv \gamma(X)(1 - P^{\varphi(R)});$$

(iv) If $P = 1$, $Q, R > 1$, then $\overline{\alpha}(X) \equiv 1 - Q^{\varphi(R)}$,
$\overline{\beta}(X) \equiv \overline{\gamma}(X) \equiv 0$;
(v) If $P > 1$, $Q = R = 1$, then $\overline{\alpha}(X) \equiv \alpha(X)$, $\overline{\beta}(X) \equiv \beta(X)$,
$\overline{\gamma}(X) \equiv \gamma(X)$;
(vi) If $P = R = 1$, $Q > 1$, then $a(X) \equiv I_2$;
(vii) If $P = Q = 1$, $R > 1$, then $a(X) \equiv 0_2$,
and φ is the Euler totient function.

Proof. As in the paper by Kanwar, Khatkar and Sharma, if $n = \prod p^d$, where p are the prime divisors of n, we present the ring $\mathbb{Z}_n$ as the direct sum of the rings $\mathbb{Z}_{p^d}$. If $a(X) \in M_2(\mathbb{Z}_n[[X]])$ is an idempotent, using the lemma for the triviality of the idempotents modulo powers of prime we can apply the latter corollary. We divide the prime divisors of n in three groups $\{p_1, \ldots, p_k\}$, $\{q_1, \ldots, q_l\}$ and $\{r_1, \ldots, r_m\}$ depending on the form of the projection of $a(X)$ in $M_2(\mathbb{Z}_{p^d}[[X]])$:
$p \in \{p_1, \ldots, p_k\}$ if $a_i(X) \in M_2(\mathbb{Z}_{p_i^{d_i}}[[X]])$ is of the form

$$a_i(X) = \begin{pmatrix} \alpha_i(X) & \beta_i(X) \\ \gamma_i(X) & 1 - \alpha_i(X) \end{pmatrix}, \quad \alpha_i(X)(1-\alpha_i(X)) = \beta_i(X)\gamma_i(X).$$

$p \in \{q_1, \ldots, q_l\}$ or $p \in \{r_1, \ldots, r_m\}$ if the projection is, respectively, the identity matrix and the zero matrix.

Let $P = p_1^{d_1} \cdots p_k^{d_k}$, $Q = q_1^{e_1} \cdots q_l^{e_l}$, $R = r_1^{f_1} \cdots r_m^{f_m}$. The image of $a(X)$ in $M_2(\mathbb{Z}_P[[X]]) \cong M_2(\mathbb{Z}_{p_1^{d_1}}[[X]]) \oplus \cdots \oplus M_2(\mathbb{Z}_{p_k^{d_k}}[[X]])$ is of the form

$$a_i(X) = \begin{pmatrix} \alpha_i(X) & \beta_i(X) \\ \gamma_i(X) & 1-\alpha_i(X) \end{pmatrix}, \quad \alpha_i(X)(1-\alpha_i(X)) = \beta_i(X)\gamma_i(X).$$

If we choose the images of $\alpha(X), \beta(X), \gamma(X)$ modulo $p_i^{d_i}$, we can find their images modulo P using the Chinese reminder theorem. The images of $a(X)$ in
$M_2(\mathbb{Z}_Q[[X]]) \cong M_2(\mathbb{Z}_{q_1}[[X]]) \oplus \cdots \oplus M_2(\mathbb{Z}_{q_l}[[X]])$ and
$M_2(\mathbb{Z}_R[[X]]) \cong M_2(\mathbb{Z}_{r_1}[[X]]) \oplus \cdots \oplus M_2(\mathbb{Z}_{r_m}[[X]])$ are, respectively, equal to the identity matrix and the zero matrix. Since P, Q and R are pairwise coprime, it is sufficient to check whether the form of $a(X)$ given in the cases (i) – (vii) in the theorem satisfy the required conditions modulo P, Q and R.

We shall check this for $\overline{\alpha}(X)$ in the case (i) only. The other cases are handled similarly. Since $\varphi(Q), \varphi(R) \geq 1$, obviously

$$\overline{\alpha}(X) \equiv (\alpha(X)+(1-\alpha(X))P^{\varphi(Q)})(1-(PQ)^{\varphi(R)}) \equiv \alpha(X) \,(\text{mod } P).$$

By the Euler-Fermat theorem $P^{\varphi(Q)} \equiv 1 \,(\text{mod } Q)$. Hence

$$\overline{\alpha}(X) \equiv (\alpha(X) + (1 - \alpha(X)) \equiv 1 \,(\text{mod } Q),$$

and in a similar way we establish that $\overline{\alpha}(X) \equiv 0 \,(\text{mod } R)$.

Appendix

During the talk Claudio Procesi made the remark that the Quillen-Suslin theorem implies that if F is a field and X is a finite set of commuting variables, then the idempotents in $M_d(F[X])$ are diagonalizable. We present elementary arguments to confirm this fact.

Recall that the A-module M, where A is a ring, is *projective* if M is a direct summand of a free A-module, i.e. there exists another A-module N such that the module $M \oplus N$ is isomorphic to the direct sum of several (maybe an infinite number of) copies of the ring A considered as an A-module.

The Serre conjecture

In 1955 Serre made the following remark known as the *Serre conjecture*:
It is not known whether there exist projective A-modules of finite type which are not free. (On ignore s'il existe des A-modules projectifs de type fini qui ne soient pas libre.) Here $A = F[X]$ where F is a field and X is a finite set of variables.
J.-P. Serre, Faisceaux algébriques cohérents, Ann. Math. (2) **61** (1955), 197-278.

In 1976 Quillen and Suslin confirmed into affirmative the Serre conjecture.

D. Quillen, Projective modules over polynomial rings, Invent. Math. **36** (1976), 167-171.

A.A. Suslin, Projective modules over a polynomial ring are free (Russian), Dokl. Akad. Nauk SSSR **229** (1976), 1063-1066. Translation: Sov. Math., Dokl. **17** (1976), 1160-1164.

The Quillen-Suslin theorem

If A is a principal ideal domain and $|X| < \infty$, then every finitely generated projective $A[X]$-module is free.

Lemma

Let ε be an idempotent in the ring $\mathrm{End}(A^d)$ of endomorphisms of the free d-generated A-module A^d. Then

$$A^d = \mathrm{Ker}(\varepsilon) \oplus \mathrm{Im}(\varepsilon)$$

and ε acts on $\mathrm{Im}(\varepsilon)$ as the identity map.

Proof. Every $v \in A^d$ can be written in the form $v = (1-\varepsilon)v + \varepsilon v$. Since $\varepsilon^2 = \varepsilon$ we obtain that $\varepsilon((1-\varepsilon)v) = 0$ and $\varepsilon(\varepsilon v) = \varepsilon v$. Hence ε acts as the identity map on $\mathrm{Im}(\varepsilon)$ and $A^d = \mathrm{Ker}(\varepsilon) + \mathrm{Im}(\varepsilon)$. It is easy to see that $\mathrm{Ker}(\varepsilon) \cap \mathrm{Im}(\varepsilon) = 0$ which implies that $A^d = \mathrm{Ker}(\varepsilon) \oplus \mathrm{Im}(\varepsilon)$.

Theorem

Let A be a principal ideal domain and let $|X| < \infty$. Then for all d every idempotent matrix in $M_d(A[X])$ is diagonalizable with eigenvalues equal to 0 and 1.

Proof. Let us consider the idempotent $a \in M_d(A[X])$ as the matrix of a linear operator ε in the d-generated free $A[X]$-module $A[X]^d$ with basis $\{v_1, \ldots, v_d\}$. By the lemma $A[X]^d = \mathrm{Ker}(\varepsilon) \oplus \mathrm{Im}(\varepsilon)$ and ε acts on $\mathrm{Im}(\varepsilon)$ as the identity map. By the Quillen-Suslin theorem both $\mathrm{Ker}(\varepsilon)$ and $\mathrm{Im}(\varepsilon)$ are free $A[X]$-modules. We fix bases $\{w_1, \ldots, w_m\}$ and $\{w_{m+1}, \ldots, w_d\}$ of $\mathrm{Ker}(\varepsilon)$ and $\mathrm{Im}(\varepsilon)$, respectively. Then the matrix b of ε with respect to the basis $\{w_1, \ldots, w_d\}$ is diagonal with eigenvalues 0 and 1 only. Clearly the matrices a and b are similar and hence a is diagonalizable.

Corollary

Let $A = A_1 \oplus \cdots \oplus A_s$ be a direct sum of a finite number of principal ideal domains $A_1, \ldots, A_s$ and let $|X| < \infty$. Then every idempotent matrix in $M_d(A[X])$ is diagonalizable.

The proof follows immediately from the theorem because a matrix in $M_d(A[X])$ is diagonalizable if and only if its projections on $M_d(A_i[X])$ are diagonalizable for all $i = 1, \ldots, s$.

Corollary

Let $n > 1$ be a square-free integer and let $|X| < \infty$. Then every idempotent matrix in $M_d(\mathbb{Z}_n[X])$ is diagonalizable.

Again, the proof is straightforward because if $n = p_1 \cdots p_s$ is square-free, where p_i are the prime factors of n, then $\mathbb{Z}_n$ is a direct sum of the prime fields $\mathbb{Z}_{p_i}$, $i = 1, \ldots, s$.

Remark

If A is a direct sum of principal ideal domains then the eigenvalues of the idempotent matrices in $M_d(A[X])$ may be different from 0 and 1 and the diagonal form may be not unique.

Example (eigenvalues different from 0 and 1)

Let $A = \mathbb{Z}_6 \cong \mathbb{Z}_2 \oplus \mathbb{Z}_3$ and

$$a = \begin{pmatrix} 3(1+x) & 3(1+x) \\ 3x & 3x \end{pmatrix} \in M_2(\mathbb{Z}_6[x]), a^2 = a,$$

$$c = \begin{pmatrix} 1+3x & 3 \\ 3x & 1 \end{pmatrix} \in GL_2(\mathbb{Z}_6[x]), b = c^{-1}ac = \begin{pmatrix} 3 & 0 \\ 0 & 0 \end{pmatrix}.$$

Example (the diagonal form is not unique)

Let $A = \mathbb{Z}_6 \cong \mathbb{Z}_2 \oplus \mathbb{Z}_3$ and

$$a = \begin{pmatrix} 1+x & 1+x \\ 5x & 5x \end{pmatrix} \in M_2(\mathbb{Z}_6[x]), a^2 = a,$$

$$c_1 = \begin{pmatrix} 1+x & 5 \\ 5x & 1 \end{pmatrix} \in GL_2(\mathbb{Z}_6[x]), b_1 = c_1^{-1} a c_1 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix},$$

$$c_2 = \begin{pmatrix} 1+3x & 1+4x \\ 2+3x & 3+2x \end{pmatrix} \in GL_2(\mathbb{Z}_6[x]), b_2 = c_2^{-1} a c_2 = \begin{pmatrix} 3 & 0 \\ 0 & 4 \end{pmatrix}.$$