Balanced Factorizations

Wuthrich, Zachary

June 2017

Contents

1 Introduction

1.1 The Problem

This problem was invented by Anton N. Vassilyev, and it was first presented to the public at the Kazakhstan republican mathematical olympiad for high-school students in 2013 [2]. The problem was, ”Prove that any rational number can be factored into a product of several rationals whose sum vanishes.”

This problem is more straightforward than one might expect. For example, consider the factorization of a rational number $a = \frac{a}{2} * \frac{a}{2} * (-a) * \frac{2}{a} * \frac{-2}{a}$ into five factors. Howevever, not all balanced factorizations are so simple minded. When I first saw the general form for the balanced factorization of some rational number into four factors I almost cried. Just for fun, here is that horrendous formula:

$$x = \tfrac{2(1-4xy^4)^2}{3y(1+8xy^4} \cdot \tfrac{-(1+8xy^4)}{6y} \cdot \tfrac{-(1+8xy^4)}{2y(1-4xy^4} \cdot \tfrac{18xy^4}{y(1-4xy^4)(1+8xy^4)}$$

Where $xy^4 \notin \{1/4, -1/8, 0\}$ [1]. Rather than going in depth into finding equations like these, there are two more interesting but closely related questions that I will examine in more detail: What is the possible number of factors in these special factorizations, especially in different types of fields? How can we extend this to more abstract algebras? First, a definition:

Definition 1.1. A Balanced Factorization means $a \in R$, where R is a ring, can be factored into the form $a = a_1 * a_2 * \cdots * a_k$ such that $\sum_{n=1}^{k} a_j = 0$.

If we have the number of factors $k \geq 2$ and we have an algebraically closed field (every polynomial has a root), it is very easy to see that we have a balanced decomposition of any element of the field. Indeed, for a given a and k, we need to find $a_1, \cdots, a_k$ such that $a = a_1 \cdots a_k$ and $a_1 + \cdots + a_k = 0$. Then the solution is simply $a_1 = \cdots = a_{k-2} = 1$ and you can find a_k and $a_{k-1} = 2 - k - a_k$ from the quadratic equation $a_{k-1}(2 - k - a_k) = a$. This solution exists because a is an element of an algebraically closed field.

1.2 Rings and Fields

I will only briefly touch on the definition of a field, as the reader should be familiarized with this concept. A field is a set on which we can define addition and multiplication, along with an additive identity and a multiplicative identity. There should also be additive and multiplicative inverses, and the field can be associative, commutative, and distributive. A ring is almost identical to a field, but there is not necessarily a multiplicative inverse.

Definition 1.2. The Order of a Finite Field q means that the field $\mathbb{F}_q$ has q elements, $q \in \mathbb{N}$.

Definition 1.3. The Characteristic of a Finite Field k means that $1 \cdot k = 0$, where the operation "$\cdot$" means add 1 k times, and does not refer to the multiplicative operator of the group. We say the characteristic is zero when the field is not finite, and when there does not exist a $k > 0$ such that $1 \cdot k = 0$ is satisfied.

It can be shown, fairly quickly, that the characteristic of any finite field must be prime. The proof for this is not necessary for this paper, but this should be taken as a fact.

Lemma 1.1. *[4]*

Let $\mathbb{F}$ be a finite field, and let $\mathbb{G} \subset \mathbb{F}$ also be a finite field with q elements. We can consider $\mathbb{F}$ to be a vector space over $\mathbb{G}$ of dimension k (dimension should have been defined in a previous linear algebra course). Then, $\mathbb{F}$ has q^k elements.

Proof. As $\mathbb{F}$ is a vector space of dimension k, we can represent any element $\mathbf{f} \in \mathbb{F}$ using a basis over $\mathbb{G}$, $\mathbf{f} = g_1\mathbf{v}_1 + \cdots + g_k\mathbf{v}_k$, where $g_i \in \mathbb{G}$ and $\{\mathbf{v}_1 \ldots \mathbf{v}_k\}$ are the vectors in the basis of $\mathbb{F}$. As $\mathbb{G}$ has q elements, every $\mathbf{g}_i$ can take q different values. Basic combinatorics then tells us that $\mathbb{F}$ must have q^k elements. ■

From here we note that any finite field must have p^k elements, where p is prime. This would follow from noting that the characteristic of any field must be prime, and then using the lemma above to construct all the possible finite fields and hence show any field must have p^k elements.

Definition 1.4. An Ideal is a subgroup of a ring. An Ideal should be closed under addition, that is if you add any two elements in the ideal, you should stay in the ideal. An Ideal must also satisfy the property that any element in the ring multiplied by an element in the ideal is an element of the ideal.

Ideals are used in the construction of something called a **quotient ring**. This is a ring, with an "equivalence class." The basic idea, is that you are taking everything that is in the ideal (which is a subset of the elements in the ring), and you send these elements to zero and see what happens. The new object, the quotient ring, will still have all the properties of a normal ring as a consequence of how we defined an ideal to be a kind of "isolated" part of the ring.

Example: Consider the ring of one variable polynomials $\mathbb{R}[x]$. We can consider the quotient ring $\mathbb{R}[x]/(x^2 + 1)$. Here, $x^2 + 1$ is being sent to 0, so any polynomial that can factor out an $x^2 + 1$ would also be 0. Note this would also imply that $x^2 = -1$. This is not a property that any real polynomial has, but should be recognized as a property of the complex numbers. This quotient ring is in fact a way to construct the complex numbers.

2 Higher Level Concepts

Unfortunately, not every detail can be fully explained in this paper. Perhaps if this were a textbook, then there could be a much more in depth discussion of the advanced techniques used. Regardless, the following sections will attempt to prepare the reader for later proofs, and some of their more complicated subtleties.

2.1 Necessary Tools from Abstract Algebra

First I will state two of the major theorems used in the proof of Theorem 3.1. I will also explain many of the technical terms from abstract algebra that will be needed to understand these two proofs and much of the rest of this paper.

Theorem 2.1. *Hasse's Estimate, in the form of [2] pg 992, proved in [3].*

The number of points of an elliptic curve (i.e., a nonsingular and irreducible curve over the closure of the field projective curve of genus one) over a finite q-element field $\mathbb{F}_q$ is at least $q + 1 - 2\sqrt{q}$. In particular, *this is true for nonsingular and irreducible (over the closure of the field) cubic curves in the projective plane over $\mathbb{F}_q$.*

The proof of this theorem is beyond the scope of this paper.

An important concept here is that of an "Elliptic Curve". This is not strongly related to an ellipse, and I urge the reader to thoroughly separate the idea of an ellipse to that of an elliptic curve before reading further. A simple definition of an elliptic curve is as follows: The set of solutions to an equation of the form $Y^2 = X^3 + AX + B$, where A and B are coefficients in some field, and X and Y are variables. Ellptic curves are thus "cubic curves" as the highest power on a variable is three. In general, an algebraic curve is the set of solutions to some two variable polynomial $f(X, Y) = 0$.

In the above theorem an elliptic curve is defined as, "A nonsingular and irreducible curve over the closure of the field projective curve of genus one". This is some high level jargon, but I will attempt to supply some intuition for these more high level concepts. First of all, a "nonsingular curve" is a more precise way of saying a "nice curve." Nonsingular curves won't have cusp points or self intersections. In technical terms, a **singular point** is a point where the polynomial and all of its partial derivatives vanish. An "irreducible curve" refers to the fact that the polynomial defining the curve cannot be factored into two or more nonconstant polynomials. This property will strongly depend on the field or ring on which the polynomial is defined.

The "field projective curve of genus one" is a trickier concept to summarize so shortly ("genus one" has to do with the relation in elliptic curve has to tori, which are of genus one, meaning they have only one "hole"). For the most in depth explanation possible, a class in algebraic geometry might help. The "projective curve" has to do with projective geometry, which is really its own subject within algebraic geometry Projective geometry is less intuitive than the well known Euclidean geometry. For now, it suffices to say that in projective geometries we can make sense out of the phrase "points at infinity." More specifically projective geometries are characterized by the fact that all lines will intersect at exactly one point, including possibly a point at infinity. For more information, skip to section 2.2: Algebraic Geometry.

Theorem 2.2. *Mason-Stothers Theorem, in the form of [5]*

If 3 polynomials $x, y, z \in F[t]$ over a field $\mathbb{F}$ are coprime and $x + y + z = 0$, then either the degrees of all these polynomials are strictly less than the number of different roots of the product xyz in the algebraic closure of F, or all three derivatives x', y', and z' vanish (as polynomials).

The proof of the Mason-Stother's Theorem is available in [5].

Firstly, a "polynomial $x \in F[t]$ over a field $\mathbb{F}$" simply means x represents some polynomial (with variable t) whose coefficients are elements of $\mathbb{F}$.

Secondly, polynomials being "coprime" or "relatively prime" is very similar to integers being relatively prime. With integers, it means that the greatest common divisor of two numbers is 1. Similarly, we can make sense of a ”greatest common divisor (gcd)” for two polynomials. A divisor for two polynomials p and q will be another polynomial r such that when we take p/r and q/r, the results can be simplified to two other polynomials. Thus we define the gcd as the polynomial r (typically unique up to a constant) with the highest possible degree. Then the polynomials x, y, and z being coprime means the gcd is 1 (or in general the gcd is a polynomial of degree 0).

The ”Algebraic Closure” of a field is a simple concept. It simply means we take our field $\mathbb{F}_0$, and find another field $\mathbb{F}_1$ (the subscripts here do not represent the order or characteristic of the field, but are rather just indexing the fields) such that $\mathbb{F}_0 \subset \mathbb{F}_1$ and all polynomials with coefficients in $\mathbb{F}_1$ have roots. For example, $\mathbb{C}$, the complex numbers, is the algebraic closure of $\mathbb{R}$, the real numbers.

2.2 Algebraic Geometry

This is a very interesting subject. There was a taste of algebraic geometry in the paragraphs following Hasse's Estimate, Theorem 2.1, in order to explain the concept of an elliptic curve. However, algebraic geometry is not the main focus of this paper, so explanations will be limited to what is necessary for understanding the rest of this paper. Now I will give some definitions that will prove useful for later in this paper.

Affine space is practically $\mathbb{F}^n$ given some field $\mathbb{F}$, but has some more subtlties. For example, in affine space we simply ignore some of the vector space structures of the field, like the origin.

Definition 2.1. Projective Space, $\mathbb{P}[\mathbb{V}]$, is defined given a vector space $\mathbb{V}$ over some field $\mathbb{F}$. The definition is: $\mathbb{P}[\mathbb{V}] = \{\mathbb{V}/\{0\}\}/E$, where ”$/E$” refers to an additional equivalence relation. This equivalence relation states that any vectors $\mathbf{v}_0, \mathbf{v}_1 \in \mathbb{V}$ satisfying $\mathbf{v}_0 = \lambda \mathbf{v}_1$, where λ is some non-zero scalar, are defined to be equivalent vectors.

This definition can be generalized so that instead of dealing with a vector space we deal with something called a ”module.” This is analogous to a vector space, but instead of being over a field it is over a division ring (a ring such that every element has a multiplicative inverse).

Another important concept is that of **homogeneous coordinates**. Just as Euclidean space uses Cartesian coordinates, projective space uses homogeneous coordinates. Homogeneous coordinates can be used to define the ”projective curve” given some curve defined in Cartesian coordinates. The projective curve is one special case of something called a ”projective variety.”

Definition 2.2. A Projective Variety over an algebraically closed field $\mathbb{F}$ is a subset of an n dimensional projective space $\mathbb{P}^n$ over $\mathbb{F}$ that is some zero locus of a finite family of homogeneous polynomials of n+1 variables with coefficients in $\mathbb{F}$ (that generates a prime ideal). When the dimension of the projective variety is one, we call it a ”projective curve.”

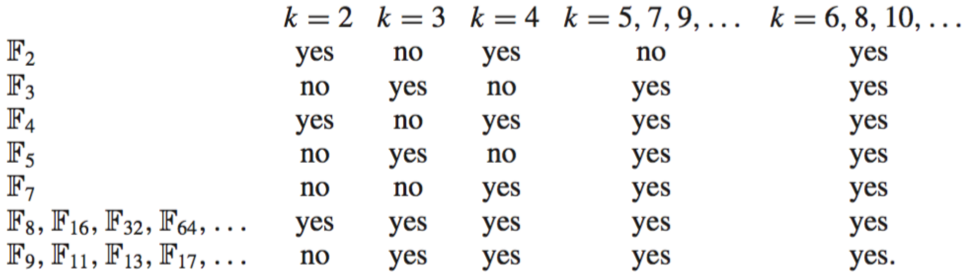
As a reminder, ”homogeneous polynomials” means that the degree of all the non-zero terms are the same. For example, $xy^5 - x^6 + x^3y^3$ is a homogeneous polynomial of degree 6. The ”zero-locus” of the polynomial is the set of points where the polynomial vanishes.

3 Balanced Decompositions in the Fields

The following theorem is a complete description of when a balanced decomposition is possible in a given finite field. Notice that the order of the field is always of the form $q = p^n$, where p is a prime and n an integer. Four different cases will be examined to complete our understanding of when a balanced decomposition is possible, and each case will have its own sub-cases that may use many different strategies to complete the proof. Some are straight forward, possibly finding the number of balanced decompositions by checking all the products in some small finite field. Other methods are less direct, utilizing the tools of abstract algebra described in section 2.

3.1 Decompositions Into k Products

Theorem 3.1. *Suppose that $k \in \mathbb{N}$, $k \geq 2$, and that $\mathbb{F}_q$ is a finite field of order q. Then in $\mathbb{F}_q$, any element can be decomposed into a product of k factors whose sum vanishes if and only if at least one of the conditions labelled ”yes” in the table below is satisfied.*



	$k=2$	$k=3$	$k=4$	$k=5,7,9,\ldots$	$k=6,8,10,\ldots$
$\mathbb{F}_2$	yes	no	yes	no	yes
$\mathbb{F}_3$	no	yes	no	yes	yes
$\mathbb{F}_4$	yes	no	yes	yes	yes
$\mathbb{F}_5$	no	yes	no	yes	yes
$\mathbb{F}_7$	no	no	yes	yes	yes
$\mathbb{F}_8, \mathbb{F}_{16}, \mathbb{F}_{32}, \mathbb{F}_{64}, \ldots$	yes	yes	yes	yes	yes
$\mathbb{F}_9, \mathbb{F}_{11}, \mathbb{F}_{13}, \mathbb{F}_{17}, \ldots$	no	yes	yes	yes	yes.

Copy of table from source [2]

This proof is one of the the main subjects of [2]. I will give at least a summary for all of the possible cases, and go into more detail for the more exciting cases.

Proof. Theorem 3.1

Case 1: k = 2. A balanced decomposition exists if and only if the characteristic of the field is 2.

The characteristic of a field is two if and only if every element of the field is square. In any field of characteristic two, if you add a number to itself, then the sum vanishes. So, when the characteristic is two, every element can be decomposed into two identical elements, and their sum will vanish. When the characteristic is not two, this will not always be possible as not every element is a square.

Case 2: k = 3. A balanced decomposition exists for every element of the field if and only if the order is 3, 5, or $\geq$ 8

When the characteristic is 3, elements turn out to be cubes, and this quickly results in a balanced decomposition. Things start to get more interesting if we say the characteristic is not 3. We have a system of equations, shown below, that we need to solve for in order to have a balanced decomposition.

$$\begin{cases} x+y+z=0 \\ xyz=a \end{cases} \tag{1}$$

This is over some finite field $\mathbb{F}_q$, where q is the order, and we want a solution to exist $\forall\ a \in \mathbb{F}_q$. Combining the equations correctly, this is equivalent to solving for at least one solution of

$$xy(x+y)=-a. \tag{2}$$

We can change this to homogeneous coordinates, and I just need the reader to trust that the resulting homogeneous polynomial will be

$$XY(X+Y)=-aZ^3. \tag{3}$$

It will prove useful to find the singular points of equation (3). This means finding where it and its partial derivative vanish. so we are trying to solve

$$\begin{cases} XY(X+Y)=-aZ^3 \\ 2XY+Y^2=0 \\ 2XY+X^2=0 \\ -3AZ^2=0 \end{cases} \tag{4}$$

Solving the system of equations (4) and keeping in mind that the characteristic is not three shows that $X=Y=Z=0$, proving there are no non-zero solutions. According to [2] this implies equation (3) has no singular points over the closure of the field $\mathbb{F}_{q\neq 3}$, and that this immediately implies the curve is irreducible and elliptic. All the conditions for Hasse's estimate have been met, and applying it shows that equation (3) has more than three points if the characteristic of the field is not three and if $q \geq 8$. The next claim in [2] is that this implies equation (2) has at least one solution, finishing the proof for $q \geq 8$. The proof for when the order of the field is 2, 4, 5, and 7 still needs to be completed.

There is no balanced decomposition for 1 if $q=2$, because in $\mathbb{F}_2$, $1+1+1=1$.

If $q=4$, 1 is the only element with a balanced decomposition. This is because in $\mathbb{F}_4$, any element x satisfies $x+x=0$ because the characteristic is two. This implies all factors must differ from each other, and because we are considering the case with 3 factors, it must be the product of the three non-zero elements of $\mathbb{F}_4$. This product equals 1.

In $\mathbb{F}_5$, the system of equations (1) has the general solution $x = y = b$, $z = -2b$, where b is the cubic root of $\frac{-a}{2}$. This works because when q=5, every element is a cube [2] pg 993.

I claim $\mathbb{F}_7$ has no balanced decomposition for $k = \pm 3$ factors. First, consider the case where any two factors are the same. Without loss of generality, take $y = x$. Then the system of equations (1) gives us $\mp 3 = 2x^3$. However, the cubes in $\mathbb{F}_7$ are 0 and ± 1 [2] pg 994. If $y = -x$ or if $y = 7 - x$, then the only way for the sum of the factors to vanish is if $z = 0$. Then their product cannot equal 3. So, there are only four cases left (weeding out the cases where the sum does not vanish). Going through each case individually: $(-1) * (-2) * 3 = 6 \neq \pm 3$, $\quad 1 * 2 * (-3) = 1 \neq \pm 3$, $\quad (-4) * 5 * 6 = 6 \neq \pm 3$, $\quad 4 * (-5) * (-6) = 1 \neq \pm 3$.

Case 3: k = 4. A balanced decomposition exists in all finite fields except of order 3 and 5.

The case for $q \geq 8$ follows the same format as in case three, but we automatically set one of the factors to 1. Then for every case of order less than eight, the proofs are not enlightening, either finding the answer through more relatively simple case work, or using brute force and calculating products.

Case 4: k $\geq$ 5. A balanced decomposition exists except when q=2 and k=5.

The general formula

$$(-1)^n \cdot a = \frac{a}{2} \cdot \frac{a}{2} \cdot (-a) \cdot \frac{2}{a} \cdot \frac{-a}{2} \cdot (1)^n \cdot (-1)^n \tag{5}$$

holds when the characteristic of the field is not two. This gives a balanced decomposition into $k = 5 + 2n$, where n is any positive integer or 0. Note that if the LHS is -a, as a is arbitrary, -a can obtain any value in the field. A balanced factorization of any element b in some field of characteristic not equal to two into $k = 6 + 2n$ factors can be obtained by the general formula

$$(-1)^n \cdot b = (-1)^n \cdot (c^2 - ca) = \frac{a}{2} \cdot \frac{a}{2} \cdot (c - a) \cdot \frac{2}{a} \cdot \frac{-2}{a} \cdot (-c) \cdot (1)^n \cdot (-1)^n$$

where c is an element such that $0 \neq c^2 \neq b$, and $a = \frac{c^2 - b}{c}$. (Such a c exists, except in the case where the field is $\mathbb{F}_3$ and $b = 1$; in this exceptional case we can take the factoring $b = 1 = 1^6$) [2] pg 994.

When the order of the field is two, we need to find balanced decompositions for -1, 0, and 1. These factorizations should be clear, with the understanding that there will need to be two formulas for when there are an odd number or even number of products. ■

One of the strongest methods used in the proof of theorem 3.1, case 4, was the creation of a "general" or "universal" formula that immediately produces a balanced decomposition in most finite fields. Taken from [1], as seen in the introduction, a balanced decomposition into 4 factors is given for most fields (this was a valid formula for when the characteristic was not 2 or 3, and if the order was not 5). The next theorem proves the search for a universal formula for a balanced decomposition into three factors is hopeless. The proof is given in [2], but be warned it is not well stated. There are many obscurities, and I will simply give an outline of the proof here.

Theorem 3.2. *[2] Theorem 3 pg 995-996*

For any field F, the element t of the field of rational fractions F[t] does not, in general, admit a balanced decomposition into a product of three factors.

The proof for this theorem contains more concepts in abstract algebra than can be presented in this paper. To ease any distress this may cause to the reader, I will simply give an outline of the proof.

Assuming that the element t^s can produce a balanced decomposition into a product of three factors, finding a common denominator for the factors would produce the identity

$$t^s = \frac{x(t)}{v(t)} \cdot \frac{y(t)}{v(t)} \cdot \frac{z(t)}{v(t)},\ \textit{where } x, y, z \in F[t],\ \textit{and } x + y + z = 0.$$

If the above equality implies $s \neq 1$, then this would show that the element t, in general, cannot be expressed as product of three terms whose sum vanishes. The actual proof in [2] attempts to prove that in fact s is a multiple of three.

Applying the Theorem 2.1, the Mason-Stothers Theorem, one can see that either the degree of the product of polynomials xyz is less than or equal to three times the degree of v. This would imply that $s = 0$. Then, according to the Mason-Stothers theorem, the other possibility is that the derivative of all of the polynomials vanish. This is only possible in finite fields. For example, examine the polynomial $4t^5 + t^{10} - 2t^{15}$ with coefficients in the finite field of order five. Then when the derivative operator is applied, all of the coefficients will become multiples of five, and hence vanish. A proof by induction is then used to prove that s must be a multiple of three.

4 The Long Awaited Algebras

An Algebra over a field is simply a general vector space equipped with a special product. We call an Algebra a unital Algebra if has an identity element with respect to multiplication.

4.1 Theorems

Lemma 4.1. *[2] pg 996.*

Suppose that the value of a one-variable polynomial over an associative commutative ring with unity at some point d is nilpotent and the value of the derivative at this point is invertible. Then the polynomial has a root in this ring. Moreover, for some root b, the difference d - b is divisible by f(d).

"Nilpotent" means that when raised to some power the result vanishes. That is, if f is our polynomial, then the "value $f'(d)$ is nilpotent" means that $(f'(d))^s = 0$, for some $s > 1$. A point being "invertible" means that there is another point such that the product of these two points is unity.

Proof. We can apply a quick change of variables such that $d = 0$, and proceed without any loss of generality from there. In general, we can write a polynomial over a ring R as

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n,$$

where, bases off the assumptions of the lemma, a_1 is invertible and $a_0^s = 0$. The proof in [2] follows an argument by an induction on s and seeks to prove that f has a root divisible by a_0.

In the quotient ring $\widetilde{R} = R/(a_0^{s-1}R)$, the image $\widetilde{f}$ of f has a root $\widetilde{c}\widetilde{a_0}$ by the induction hypothesis. Take some preimage $c \in R$ of the element $\widetilde{c} \in \widetilde{R}$, and the goal is now to find a root b of f. We can generalize b to be in the form $b = ca_0 + ta_0^{s-1}$, where t is some unknown element of R. By the nilpotent hypothesis, $a_0^s = 0$, and hence we have

$$f(b) = a_0 + a_1(ca_0 + ta_0^{s-1}) + \cdots + a_n(ca_0 + ta_0^{s-1})^n = f(ca_0) + a_1 t a_0^{s-1}. \tag{6}$$

Recognizing that ca_0 is a root of f modulo the ideal $a_0^{s-1}R$, it is true then that $f(ca_0) \in a_0^{s-1}R \Rightarrow f(ca_0) = ra_0^{s-1}$ for some $r \in R$. Note that in equation (5) $f(b) = 0$ if we take $t = -r/a_1$. ■

This is the end of the proof in [2]. I feel the induction was not made explicit, which is what makes the proof the hardest to understand. Given this lemma, it is possible to prove the following theorem.

Theorem 4.2. *[2] pg 997.*

Let $\mathbb{F}$ be a field and let n be an integer larger than two. If, in all finite extensions of $\mathbb{F}$, each element has a nonpower balanced decomposition into a product of n elements, then the same is true for each element of each finite-dimensional associative unital algebra over F.

A "nonpower" balanced decomposition means that at least one of the factors in the product is different from at least one other factor in the product. The proof for this theorem will not be given here, but if the reader is extra curious, the proof is available in [2], Theorem 4, page 997.

Corollary 4.2.1. *[2] pg 998.*

Each element of a finite dimensional unital algebra (over a field) decomposes into a product of

a) three elements whose sum vanishes if the field is algebraically closed.

b) five elements whose sum vanishes if the charactersitic of the field is not two.

Proof. (a) follows almost immediately from theorem 4.2. Simply note that in an algebraically closed field, each element has a nonpower balanced decomposition into a product of three factors. This was shown in the introduction, under definitition 1.1.

(b)To prove this, apply theorem 4.2 and theorem 3.1 case 4, and note that equation (5) always gives a nonpower decomposition. ■

Corollary 4.2.2. *[2] pg 998.*

For any $k \geq 3$, any complex or real matrix can be decomposed into a product of k matrices (over the same field) whose sum vanishes.

Proof. The corollary follows immediately from theorem 4.1 because each complex number a has a nonpower balanced decomposition into $k \geq 3$ factors:

$$a = x \cdot (x+1) \cdot 1^{k-3} \cdot (2-k-2x),$$

and this equality is a cubic equation with respect to x.

■

4.2 Examples and Special Cases

This section is meant to show that the conditions for the theorems and corollaries of section 4.1 (the previous section) are necessary conditions.

Example 1: Each element of $\mathbb{F}_3$, the field of order 3, has a balanced decomposition into three factors (this was already proved). However, consider the ring of one variable polynomials with coefficients in $F_3[x]$. We can construct the algebra $\mathbb{F}_3[x]/(x^2)$ over this field, and I claim the element $1+x$ does not admit a balanced decomposition into three factors.

Proof. $1 = 1 \cdot 1 \cdot 1$ is the unique balanced decomposition of 1 in $\mathbb{F}_3$ (This check is left to the reader as an exercise). Given this, we must have that $1+x = (1+ax)(1+bx)(1+cx)$, $a, b, c \in \mathbb{F}_3$. Expanding the RHS and applying the equivalence relation $x^2 \to 0$ we have that $1+x = 1+(a+b+c)x \;\Rightarrow\; a+b+c = 1$. It is therefore impossible for the decomposition to be balanced, as the x term will not vanish. ■

This example shows that the word "nonpower" in theorem 4.2 is necessary.

Example 2: In the algebra of polynomials F[x] over any field, the element x has no balanced decompositions. Note that the dimensionality of the vector space that the algebra is defined over is not finite-dimensional. This statement is simple enough to not require a proof. This example is meant to show that the finite-dimensionality condition of theorem 4.2 and corollary 4.2.1 cannot be omitted.

Example 3: In the field of complex numbers (which is of characteristic 0), any nonzero element has a nonpower balanced decomposition into a product of two factors.

Proof. We can create a general formula for the balanced decomposition of a nonzero complex number $z_0 = r_0 e^{i\theta_0}$. Let the balanced decomposition into two factors be $z_0 = (r_0^{1/2} e^{-i\theta_0/2})(-r_0^{1/2} e^{-i\theta_0/2})$. Locally, this always makes sense. ■

However, as you may remember from a previous linear algebra course, there exists something called the ”Nilpotent Jordan Block J.” From linear algebra (proof not provided), we know that this object J is not square, implying that -J is not square as well. Then J cannot have a balanced factorization into two products (over any field), because then that would imply that -J is square [2] Example 3, pg 999. This example shows that $k \nleq 2$ in corollary 4.2.2 is necessary, and in corollary 4.2.1 a), we cannot replace ”three” with ”two.”

Example 4: In the field $\mathbb{F}_2$, the identity element 1 does not have a balanced decomposition into a product of five factors. This has already been proven. This very simple example shows that the statement that the ”characteristic of the field is not two” in corollary 4.2.1 b) cannot be omitted.

5 Conclusion

This topic of balanced decompositions has almost been completely exhausted. Most questions related to balanced decompositions can be answered by Theorem 3.1, giving a complete description of when any finite field can admit a balanced factorization into k products, together with theorem 4.2 and its corollaries, showing when balanced decompositions are possible in many algebras. There are still a couple open questions that come to mind, however.

Question 1: Can any element of any field admit a balanced decomposition into a product of at most four factors?

We have seen that the answer is no to this question if we replace four with three, and the answer is yes if we replace four with five, but this question still remains unanswered.

Question 2: What does occur in characteristic two? Does there exist a universal formula? Does any element of any field admit a balanced factorization?

This paper largely avoided characteristic two, but perhaps there could be interesting results if it was examined in more detail. Starting as a high school math olympiad question in Kazakhstan, the question of balanced decompositions turned out to be a quite involved mathematical problem, utilizing many complex mathematical concepts in both abstract algebra and algebraic geometry.

References

[1] Klyachko, A. A., Mazhugg, A. M., Ponfilenko, A. N., Balanced Factorisations in some algebras (2016), http://arxiv.org/abs/1607.01957.

[2] Klyachko, Anton A., and Vassilyev, Anton N. “Balanced Factorizations.” The American Mathematical Monthly, vol. 123, no. 10, 2016, pp. 989–1000. JSTOR, www.jstor.org/stable/10.4169/amer.math.monthly.123.10.989.

[3] Silverman, J. H., The Arithmetic of Elliptic Curves. Springer-Verlag, New York, 1986, Theorem V.I.I, pp. 138.

[4] Neunhoeffer, Max. ”Chapter 3: Finite Fields.” N.p.: n.p., 1991. 23-30. Web. 30 May 2017. http://www.math.rwth-aachen.de/ Max.Neunhoeffer/Teaching/ff/ffchap3.pdf.

[5] Snyder, N., An alternate proof of Mason’s theorem, Elem. Math. 55 no.3 (2000) 93–94.