2014

On the divided power structures in super-rings

Reginald F. Robson
University of Windsor

On the Divided Power Structures in Super-Rings

Reginald F. Robson

A Thesis

Submitted to the Faculty of Graduate Studies

through The Department of Mathematics and Statistics

in Partial Fulfilment of the Requirements for

the Degree of Master of Science at the

University of Windsor

Windsor, Ontario, Canada

2014

On the Divided Power Structures in Super Rings

by

Reginald F. Robson

APPROVED BY:

E. Kim
Department of Physics

W.L. Yee
Department of Mathematics and Statistics

I. Shapiro, Advisor
Department of Mathematics and Statistics

May 12, 2014

Author's Declaration of Originality

I hereby certify that I am the sole author of this thesis and that no part of this thesis has been published or submitted for publication.

I certify that, to the best of my knowledge, my thesis does not infringe upon anyone's copyright nor violate any proprietary rights and that any ideas, techniques, quotations, or any other material from the work of other people included in my thesis, published or otherwise, are fully acknowledged in accordance with the standard referencing practices. Furthermore, to the extent that I have included copyrighted material that surpasses the bounds of fair dealing within the meaning of the Canada Copyright Act, I certify that I have obtained a written permission from the copyright owner(s) to include such material(s) in my thesis and have included copies of such copyright clearances to my appendix.

I declare that this is a true copy of my thesis, including any final revisions, as approved by my thesis committee and the Graduate Studies office, and that this thesis has not been submitted for a higher degree to any other University or Institution.

Abstract

Abstract. Given a super-commutative ring $A = A_0 \oplus A_1$, does (A_0, A_1A_1) always have a divided power structure? We give an example proving the answer is no. There exists a super-commutative ring $SR = SR_0 \oplus SR_1$ with no divided power structure possible on (SR_0, SR_1SR_1). Also, we study super divided power structures and the properties they force onto divided power structures on the even part of a ring-ideal pair. We show that there can exist a divided power structure on the even part that is incompatible with the super divided power structure.

Also, just for fun, we explore the phenomenon of upper-Sierpinski-triangular matrices and where they manifest.

Dedication

To Amie, thanks for putting up with all this.

Acknowledgements

I would like to acknowledge my supervisor Ilya Shapiro. Without his support and guidance this thesis would not exist. Also, thanks to all the math professors at the University of Windsor, it has truly been a pleasure studying with you.

Contents

CHAPTER 1

Introduction

In 2006 a question arose from a paper by Albert Schwarz and Ilya Shapiro[**17**]. Schwarz and Shapiro recognized that many super-rings have divided power structures even when the analogous commutative rings have none. For example $\big(\mathbb{Z}[x,y],(xy)\big)$ does not have a divided power structure as there is generally no way to divide, but it's analogous super-ring $\big((\mathbb{Z}[\xi_1,\xi_2])_0\,,(\xi_1\xi_2)\big)$ does have a divided power structure, since the powers of the nilpotent elements are zero, and zero is the only integer that may be divided by any other integer and remain an integer.

In this thesis we give an example of a $\mathbb{F}_p$ super-algebra $A = A_0 \oplus A_1$ with no divided power structure on the ideal A_1A_1, answering the question in the negative. There are super-rings without divided power structure. Before getting to the example, as an introduction we shall go over the mathematical history that led to the question being asked in the first place.

1.1. De Rham Cohomology

De Rham cohomology was (somewhat paradoxically) discovered before cohomology as Georges de Rham demonstrated it in his thesis in 1931 while the idea for cohomology was introduced by Andrey Kolmogoroff and J.W. Alexander independently at the topology conference in Moscow in 1935 [**13**, p. 801, 731]. De Rham wrote his theorem in terms of homology groups. It was only in the years after the introduction of cohomology theory that it was recognized as an antecedent, the premonition of what was to come [**13**, p. 580].

De Rham was responding to a conjecture made by Elie Cartan dealing with the complex of exterior differential forms on a smooth manifold M [**13**, p. 801]. That is, something like this:

$$0 \to \Omega^0(M) \xrightarrow{d_1} \Omega^1(M) \xrightarrow{d_2} \Omega^2(M) \xrightarrow{d_3} \Omega^3(M) \xrightarrow{d_4} \cdots$$

where $\Omega^n(M)$ is the module of n-forms on M, and d is the exterior derivative[1]. Cartan's conjecture dealt with the relationship between exact and closed differential forms. An n-form, $\omega \in \Omega^n(M)$, is called *exact* if there exists an $(n-1)$-form,

[1]Today this is called the *De Rham complex.*

$\omega' \in \Omega^{n-1}(M)$, such that $d(\omega') = \omega$, while an n-form $\omega \in \Omega^n(M)$ is called *closed* if $d(\omega) = 0$. Part of the definition of a complex is the requirement that $d^2 = 0$, which implies that all exact forms are necessarily closed. The converse of this in $\mathbb{R}^n$ is erroneously referred to as the Poincaré Lemma, when it really should be attributed to Vito Volterra[2] [**7, 16**, p. 63, 526 resp.].

Poincaré Lemma. *If M is a manifold which is smoothly contractible to a point (such as $\mathbb{R}^n$), and ω is a closed form on M, then it is exact.*

The de Rham cohomology groups

$$H^n_{dR}(M) = \frac{\ker(d_n)}{\mathrm{im}(d_{n-1})}$$

measure how much a manifold fails to follow the Poincaré Lemma. That is, in what way closed forms on M are or are not exact.

De Rham proved Cartan's Conjecture, by showing what is now known as:

De Rham's Theorem. *Let M be a smooth manifold, let $\Delta^n(M)$ be the free abelian group generated by the n-simplices and let $H^n(M;\mathbb{R})$ be the n^{th} simplicial cohomology group. The homomorphism*

$$\Psi : \Omega^n(M) \to \Delta^n(M)$$

where $\Psi(\omega) : \Delta_n(M) \to \mathbb{R}$ is given by

$$\Psi(\omega)(\sigma) = \int_\sigma \omega$$

induces an isomorphism

$$\Psi^* : H^n_{dR}(M) \to H^n(M;\mathbb{R}) \ .$$

Here are some examples of de Rham cohomology that will be important to keep in mind as we continue.

Example 1. *De Rham cohomology of a point.* A function from a point x to $\mathbb{R}$ is completely defined by its value at x. It is obviously a constant function. So we have $\Omega^0(x) = \mathbb{R}$, and for $n \geq 1, \Omega^n(x) = 0$. So our complex looks like:

$$0 \longrightarrow \mathbb{R} \longrightarrow 0 \longrightarrow \cdots \ .$$

Thus $H^0_{dR}(x) = \mathbb{R}$, and for $n \geq 1, H^n_{dR}(x) = 0$.

Example 2. *De Rham cohomology of a line.* The set of smooth functions from a line l to $\mathbb{R}$ is just C^∞ from the undergrad days. We have $\Omega^0(l) = C^\infty$, $\Omega^1(l) = C^\infty dx$,

[2]Of course, since it has been called that for almost a century, to call it anything else now would lead to confusion. We can not beat them, so we will join them.

and for $n \geq 2$, $\Omega^n(l) = 0$. Giving us a complex:

$$0 \longrightarrow C^\infty \xrightarrow{d_1} C^\infty dx \xrightarrow{d_2} 0 \longrightarrow \cdots .$$

So $H^0_{dR}(l) = \ker(d_1) \simeq \mathbb{R}$, since the derivative kills only the constant functions. Next we need to find $H^1_{dR}(l) = \dfrac{\ker(d_2)}{\mathrm{im}(d_1)}$. Obviously $\ker(d_2) = C^\infty dx$, and the Fundamental Theorem of Calculus gives us for every smooth function f, we have $F(x) = \int_0^x f(t)dt$ is a smooth function with $d(F(x)) = f(x)dx$, so every function is exact and $\mathrm{im}(d_1) = C^\infty dx$. So $H^1_{dR}(l) = \dfrac{\ker(d_2)}{\mathrm{im}(d_1)} = \dfrac{C^\infty dx}{C^\infty dx} = 0$.

Example 3. *De Rham cohomology of a circle.* The set of smooth functions from a circle S^1 to $\mathbb{R}$ is isomorphic to the set of smooth periodic functions with period length P. We shall use the symbol C^∞_P to represent this set of functions. We now have $\Omega^0(S^1) = C^\infty_P$, $\Omega^1(S^1) = C^\infty_P dx$, and for $n \geq 2, \Omega^n(S^1) = 0$. Giving us a complex:

$$0 \longrightarrow C^\infty_P \xrightarrow{d_1} C^\infty_P dx \xrightarrow{d_2} 0 \longrightarrow \cdots .$$

As before $H^0_{dR}(S^1) = \ker(d_1) \simeq \mathbb{R}$, as the functions killed by d_1 are exactly the constant functions. Now $H^1_{dR}(S^1) = \dfrac{\ker(d_2)}{\mathrm{im}(d_1)}$, and we know $\ker(d_2) = C^\infty_P dx$, but what is $\mathrm{im}(d_1)$? A form $f(x)dx \in C^\infty_P dx$ is exact if $F(x) = \int_0^x f(t)dt$ is in C^∞_P, which would only be true if $F(x) = F(x+P)$. So specifically, when $x = 0$ we get $\int_0^P f(t)dt = \int_0^0 f(t)dt = 0$, which is sufficient as $f(x)$ is itself P periodic. Thus $\mathrm{im}(d_1) = \{f(x)dx \in C^\infty_P dx | \int_0^P f(x)dx = 0\}$. Now, if $g(x)dx$ is not an exact form we can find a constant $c = \int_0^P g(x)dx$ such that now $(g(x) - c)dx$ is an exact form. Thus $H^1_{dR}(S^1) = \dfrac{\ker(d_2)}{\mathrm{im}(d_1)} = \mathbb{R}$.

So the line has the same cohomology as the point, but the circle does not. This is because the line is contractible to the point, while the circle is not.

The Difference between the Real and Finite Worlds: Frobenius. It is important to note that de Rham cohomology is only defined on smooth *manifolds*, which requires the ground field to be either $\mathbb{R}$ or $\mathbb{C}$. If we try to use it on a variety over the finite field $\mathbb{F}_p$, where p is a prime, then we run into trouble with our calculations. For instance, consider the 1-form $x^{p-1}dx$. Obviously it is closed, but is it exact? If our base field had characteristic 0, we could say yes, as then $d(\frac{1}{p}x^p) = x^{p-1}dx$; but since our field has characteristic p, we are not able to divide by p. Notice that in characteristic p the function $x \mapsto x^p$ is an endomorphism. This is commonly called the Frobenius endomorphism, after Ferdinand George Frobenius [**18**]. In the $\mathbb{R}$-world $x^{p-1}dx$ is a part of the cohomology of a line; in $\mathbb{F}_p$ it is not as intuitive what a "line" is but if such a thing exists we expect it to be contractible. So we want it to have the same cohomology of a point, where every closed form is also exact[3], but $x^{p-1}dx$ is a closed form that fails to be exact. The solution to this problem would not arise for at least another two decades.

1.2. Increasing Abstraction

The story of cohomology begins on manifolds, but it does not end there. Over the next few decades more cohomology theories developed, and topologists began to realize that they were, in fact, invariants of algebraic systems [**13**, p. 804]. The creation of category theory by Samuel Eilenberg and Saunders Mac Lane in 1945 was precipitated in part by a desire to connect the various homology and cohomology theories [**8, 13**, p. 911 and p. 805 resp.]. Category theory leads to extraordinary abstraction by axiomatizing essential properties of known algebraic objects and keeping only what is necessary for a given construction [**8**, p. 791]. Alexander Grothendieck developed the ideas of abelian categories and additive functors to unify the cohomology of sheaves and the cohomology of groups [**10**]. Six years later he had developed an algebraic version of de Rham cohomology which he wrote about in a letter to Michael Atiyah, (which was published in 1966) [**11**]. It was from this algebraic de Rham cohomology that Grothendieck began to develop cohomology theories for fields with positive characteristic.

1.3. Crystalline Cohomology

As we have already mentioned in 1.1, de Rham cohomology leaves something to be desired. Over fields of characteristic 0, everything works out, but in fields of positive characteristic there are problems whose situation require a different approach. There have been a number of cohomology theories developed to solve the problems. The driving motivation was provided by the Weil conjectures.

In 1949 André Weil developed four conjectures about zeta functions of algebraic varieties over a p characteristic field $\mathbb{F}_q$ analogous to the Riemann hypothesis for the Riemann zeta function [**20**]. It was know that given a sufficiently "good" cohomology theory[4] the Weil conjectures could be proven [**3**, 1.2]. The first to have success was a p-adic cohomology argument put forward by Bernard Dwork in 1960 [**9**]. It proved the first of the Weil conjectures. The next successful cohomology theory was Grothendieck's ℓ-adic cohomology, (where ℓ is any prime other than p), which led to the proofs of the next two Weil conjectures but had the drawback of killing off information about p-torsion [**3**, 1.7]. In order to keep this information crystalline

[3]That is, where the Poincaré Lemma holds.

[4]"Good" meaning satisfying the Weil cohomology axioms, which can be found in [**3**, 1.2 - 1.4].

cohomology was developed. In order to complete the Weil conjecture story we should point out that Grothendieck's student Pierre Deligne proved the final of the four Weil conjecture in 1974, the same year Pierre Berthelot, another student of Grothendieck's, completed his thesis fully defining crystalline cohomology [**5**].

The entire construction of crystalline cohomology is complicated and uses machinery such as Grothendieck's topos and a great deal of category theory to construct what is referred to as the crystalline site. This part of the theory is important for establishing crystalline cohomology as an invariant, but it does not play a direct role in our research. We are instead interested in how Berthelot got around the Frobenius problem highlighted earlier; ensuring the Poincaré Lemma (1.1) still holds in positive characteristic. The trick he used involved divided power structures [**2**].

1.4. Divided Power Structures

Divided power structures were presented by Henri Cartan in 1955 as part of the seventh Séminaire H. Cartan at the École normale supérieure in Paris [**4**]. His definition is essentially identical to the definition used by Grothendieck's student Pierre Berthelot in his thesis published in 1974 [**2**]. We will follow Berthelot's definition.

Definition 4. A divided power structure (or DP structure) is a sequence of maps (γ_n) on an ideal I of a ring R. We say that for (R, I) to have a DP structure (R, I, γ) the maps must satisfy the following rules.

1. $\forall x \in I, \gamma_0(x) = 1, \gamma_1(x) = x, \gamma_i(x) \in I$ if $i \geq 1$
2. $\forall x, y \in I, \gamma_k(x + y) = \sum_{i+j=k} \gamma_i(x)\gamma_j(y)$
3. $\forall \lambda \in R, \forall x \in I, \gamma_k(\lambda x) = \lambda^k \gamma_k(x)$
4. $\forall x \in I, \gamma_i(x)\gamma_j(x) = \frac{(i+j)!}{(i)!(j)!}\gamma_{i+j}(x)$
5. $\forall x \in I, \gamma_p(\gamma_q(x)) = \frac{(pq)!}{p!(q!)^p}\gamma_{pq}(x)$

The maps are defined in such a way as to mimic the behaviour of $\dfrac{x^n}{n!}$ in $(\mathbb{Q}[x], (x))$. With a little work it becomes clear that $k!\gamma_k(x) = x^k$ is true for all k and all $x \in I$. Notice that $d\left(\dfrac{x^n}{n!}\right) = \dfrac{x^{n-1}}{(n-1)!}dx$. So similarly, for any differential graded algebra with a DP structure we define $d\left(\gamma_n(x)\right) = \gamma_{n-1}(x)dx$. If a ring of characteristic p has such a structure our concerns about the exactness of $x^{p-1}dx$ are soothed, as $d\left(\gamma_p(x)\right) = \gamma_{p-1}(x)dx$, and since $x^{p-1} = (p-1)!\gamma_{p-1}(x) \equiv_p -\gamma_{p-1}(x)$, we know that $x^{p-1}dx$ is exact and is the image of $-\gamma_p(x)$. Divided power structures are usually notated as a triplet: (R, I, γ), the ring, the ideal, and the maps. In 1963 Norbert Roby published a construction of a $\mathbb{Z}$ graded divided power algebra $\Gamma(M)$ for any A-module M, such that $\Gamma_0(M) = A$, $\Gamma_1(M) = M$, and there is a guaranteed divided power structure [**15**]. Using this, Berthelot was able to create the construction in the following theorem. We shall call this construction the *divided power envelope*.

Theorem 5. [**3**, Theorem 3.19] *Let (A, I, γ) be a DP algebra and let J be an ideal in an A-algebra B. Then there exists a B-algebra $\mathcal{D}_{B,\gamma}(J)$ with a D.P. ideal $(\bar{J}, \varepsilon)$, such that $J\mathcal{D}_{B,\gamma}(J) \subseteq \bar{J}$, such that ε is compatible with γ, and with the following universal property: for any B-algebra C containing an ideal K which contains JC and with a DP structure δ compatible with γ, there is a unique D.P. morphism $(\mathcal{D}_{B,\gamma}(J), \bar{J}, \varepsilon) \longrightarrow (C, K, \delta)$ making the diagram commute:*

$$\begin{tikzcd}
& \big(\mathcal{D}_{B,\gamma}(J), \bar{J}, \varepsilon\big) \arrow[dr, dashed] & \\
(B, J) \arrow[ur, "\psi"] \arrow[rr] & & (C, K, \delta) \\
& (A, I, \gamma) \arrow[ul, "f"] \arrow[ur, "g"'] &
\end{tikzcd}$$

Using this construction Berthelot creates a way to "thicken" a variety V over $\mathbb{F}_p$, by taking a Zariski open neighbourhood of V which allows for a divided power structure.

1.5. Koszul-Tate Resolutions

An additional application of divided power structures is in Koszul-Tate resolutions. These are projective resolutions that were introduced by John Tate in 1957 as a generalization of the complex discovered by Jean-Louis Koszul [**19**]. The resulting complex was used by Friedemann Brandt, Glenn Barnich, and Marc Henneaux to calculate BRST cohomology, which we understand might mean something to physicists [**1**, section 5.].

Here is Tate's definition of a differential graded algebra.

Definition 6. Given a ring R, a *differential graded algebra* X is an R-algebra satisfying the following axioms.

(1) X is $\mathbb{Z}$ graded. That is $X = \bigoplus_{i\in\mathbb{Z}} X_i$, is the direct sum of R-modules with $X_iX_j \subseteq X_{i+j}$.
(2) $X_i = 0$ for $i < 0$, $X_0 = R$, and X_i is an R-module for $i > 0$.
(3) X is strictly skew-commutative[5], that is:

$$xy = (-1)^{ij}yx, \quad \text{for } x \in X_i \text{ and } y \in X_j\ .$$

[5]We would call this super-commutative.

(4) The map d is a skew derivation of degree -1, that is, $dX_i \subseteq X_{i-1}$ for all i, $d^2 = 0$, and

$$d(xy) = (dx)\, y + (-1)^i\, x\,(dy)\,, \quad \text{for } x \in X_i \text{ and } y \in X_j\ .$$

So we have a complex:

$$\cdots \xrightarrow{d_{i+1}} X_i \xrightarrow{d_i} X_{i-1} \xrightarrow{d_{i-1}} \cdots \xrightarrow{d_3} X_2 \xrightarrow{d_2} X_1 \xrightarrow{d_1} X_0 = R \longrightarrow 0$$

Notice that this is almost the same as a de Rham complex only d is going in the opposite direction. Indeed, if a de Rham complex has finite length then through changing the index we can fit such a complex into Tate's definition.

Tate is concerned with killing elements which are closed, but not exact; or more generally, elements in $ker(d_{i-1})$ that are not in $\mathrm{im}(d_i)$. In order to kill a closed element of degree $\rho - 1$ an element T of degree ρ is adjoined to our complex creating a new complex Y with the property that $d(T) = t$. The proper way to go about doing this depends on the parity of ρ. If ρ is odd, then $Y = \dfrac{X[T]}{(T^2)}$, and $Y_i = X_i + X_{i-\rho}T$. The multiplication rules around T are defined by the facts that $T^2 = 0$ and $Tx = (-1)^i xT$ for $x \in X_i$. The derivation also is forced to conform to the rule $d(xT) = (dx)T + (-1)^i xt$ for $x \in X_i$.

If ρ is even the construction gets more interesting. This is where divided powers come onto the scene. Set $Y = X\langle T\rangle$ where $X\langle T\rangle$ is the divided power polynomial ring[6], with basis elements $T^{(i)}$, where

$$T^{(i)}T^{(j)} = \frac{(i+j)!}{i!j!}T^{(i+j)}\ .$$

Notice that we have now forced a divided power structure on the ideal $\langle T\rangle$, with $\gamma_k\left(T^{(i)}\right) = T^{(i+k)}$. The grading of Y now follows the rule

$$Y_i = X_i + X_{i-\rho}T^{(1)} + X_{i-2\rho}T^{(2)} + \cdots$$

and the derivation follows the rules $d(T^{(k)}) = T^{(k-1)}t$, and $d(xT^{(k)}) = (dx)T^{(k)} + (-1)^i xT^{(k-1)}t$ for $x \in X_i$.

By repeating this process (possibly infinitely) we create a complex with all homology groups equal to zero, save the first which is equal to $\dfrac{R}{\mathrm{im}(d_1)}$ **[19]**.

1.6. Super-Commutative Rings

Without drawing attention to it we have already dealt with some super-commutative rings. The de Rham complex is an example of a differential graded algebra, as were the rings mentioned in 1.5, and DGAs are examples of super rings. Super rings are

[6] If we set $Y = X[T]$, we run into the same problem as discussed in 1.1.

defined as follows. A *super ring* is a ring R with a $\frac{\mathbb{Z}}{2\mathbb{Z}}$ grading such that $R = R_0 \oplus R_1$. In a super ring the elements of R_1 (the "odd" elements) are anti-commutative, that is

$$\forall a, b \in R_1, ab = -ba \ ,$$

and the elements of R_0 (the "even" elements) commute with everything, i.e.

$$\forall x \in R_0, \forall r \in R, xr = rx \ .$$

The prefix "super" comes from physics, as in "supergravity" and "supersymmetry"; theories that use anti-commutative Grassmann dimensions [**12**].

1.7. Our Question

In 2006 Albert Schwarz and Ilya Shapiro published a result that provides a way to avoid some of the giant machinery in crystalline cohomolog [**17**]. Rather than using Berthelot's method with the divided power envelope they created an infinitesimal "thickening" by passing into the super-world. Since the super-rings they used have a natural divided power structure, they were able to avoid the grief of the crystalline site and create a de Rham style cohomology that is easier to compute. During the refereeing process for their paper, a question came up: Given a super ring $A = A_0 \oplus A_1$ is there is always an obvious DP structure for (A_0, A_1A_1)? For example $\big(\mathbb{Z}[x_i], (x_i)\big)$ has no DP structure, but $\big((\mathbb{Z}[\xi_i])_0, (\xi_i)^2\big)$ does. As a demonstration of this take $2n$ different odd variables, $\xi_1, \ldots, \xi_{2n}$, pair them up and sum them $\xi_1\xi_2 + \cdots + \xi_{2n-1}\xi_{2n}$. Now by the multinomial theorem $(\xi_1\xi_2 + \cdots + \xi_{2n-1}\xi_{2n})^n = n!\xi_1\xi_2 \cdots \xi_{2n-1}\xi_{2n}$, so the idea of dividing powers of by $n!$ does actually make sense since any n^{th} power will be divisible by $n!$. This gives some reason to believe that super rings might always be so "nice", but this is not case. We will show an example of a super ring without this property.

CHAPTER 2

The Koblitz Example

In Berthelot and Arthur Ogus' explanation of divided power structures in [**3**] they give an example, attributed to Neil Koblitz, of a ring that only just fails to have a DP structure. They leave the proof as an exercise. Here is that exercise completed.

Let
$$K = \frac{\mathbb{F}_p[x_1, \ldots, x_6]}{(x_1^p, \ldots, x_6^p, x_1x_2 + x_3x_4 + x_5x_6)}$$
and $I = (x_1, \ldots, x_6) \subset K$. We will show that (K, I) has no divided power structure. To do this we shall assume that it does have some divided power structure γ and we will divine a contradiction.

Now, by rule 3, $\gamma_p(-x_1x_2) = x_1^p\gamma_p(-x_2) = 0$ but following divided power rule 2 we get[1],

$$\begin{aligned}
\gamma_p(-x_1x_2) &= \gamma_p(x_3x_4 + x_5x_6) \\
&= \sum_{i=0}^{p} \gamma_i(x_3x_4)\gamma_{p-i}(x_5x_6) \\
&= \sum_{i=1}^{p-1} \frac{(x_3x_4)^i}{i!} \cdot \frac{(x_5x_6)^{p-i}}{(p-i)!} \\
&= \sum_{i=1}^{p-1} \frac{(-1)^i(x_3x_4)^i(x_5x_6)^{p-i}}{i} \ .
\end{aligned}$$

We will demonstrate that $\displaystyle\sum_{i=1}^{p-1} \frac{(-1)^i(x_3x_4)^i(x_5x_6)^{p-i}}{i}$ is not zero in our ring.[2] We will consider K as a graded ring, but first some lemmas about graded rings need to be shown.

Lemma 7. *Let $R_\bullet$ be a G-graded ring where G is an abelian group, and $f \in R_k$, then*
$$\left(\frac{R_\bullet}{(f)}\right)_g = \frac{R_g}{R_{gk^{-1}}f} \ .$$

Proof. $R_\bullet$ is a G-graded ring means $R_\bullet = \bigoplus_{g\in G} R_g$, where each R_g is an abelian additive group, and $x \in R_g$, $y \in R_h \Rightarrow xy \in R_{gh}$.

[1] See Appendix A, Fact 21.

[2] Which means that γ_p is not well-defined on K.

Since $f \in R_k$, then $(f) = \{rf : r \in R_\bullet\}$. The homogeneity of f is an important restriction; it allows us to easily place homogenous multiples of f. It is because of this that $(f) = \bigoplus_{g\in G}((f) \cap R_g)$. Each of these $((f) \cap R_g)$ is the set of elements from (f) of degree g in $R_\bullet$; that is, the elements $rf,$ where $r \in R_{gk^{-1}}$so that $rf \in R_{gk^{-1}k} = R_g$.

So now,

$$\begin{aligned}
\frac{R_\bullet}{(f)} &= \{q + (f) : q \in R_\bullet\} \\
&= \bigoplus_{g\in G} \{q_g + (f) \cap R_g : q_g \in R_g\} \\
&= \bigoplus_{g\in G} \{q_g + \{rf : r \in R_{gk^{-1}}\} : q_g \in R_g\} \\
&= \bigoplus_{g\in G} \{q_g + R_{gk^{-1}} f : q_g \in R_g\} \\
&= \bigoplus_{g\in G} \frac{R_g}{R_{gk^{-1}} f} \ .
\end{aligned}$$

Thus $\left(\frac{R_\bullet}{(f)}\right)_g = \frac{R_g}{R_{gk^{-1}} f}$. □

Lemma 8. *Let $R_\bullet$ be a G-graded ring, and let I be a finitely generated ideal say $I = (f_1, \ldots, f_s)$ and $\forall i \in \{1 \ldots s\}, f_i \in R_{k_i}$. Then*

$$\left(\frac{R_\bullet}{I}\right)_g = \frac{R_g}{\sum_{i=1}^{s} R_{gk_i^{-1}} f_i} \ .$$

Proof. We know that $I \cap R_g = \left\{\sum_{i=1}^{s} r_i f_i : r_i \in R_{gk_i^{-1}}\right\}$by the same logic as lemma 7, so

$$\begin{aligned}
\frac{R_\bullet}{I} &= \{q + I : q \in R_\bullet\} \\
&= \bigoplus_{g\in G} \{q_g + I \cap R_g : q_g \in R_g\} \\
&= \bigoplus_{g\in G} \left\{q_g + \left\{\sum_{i=1}^{s} r_i f_i : r_i \in R_{gk_i^{-1}}\right\} : q_g \in R_g\right\} \\
&= \bigoplus_{g\in G} \left\{q_g + \sum_{i=1}^{s} R_{gk_i^{-1}} f_i : q_g \in R_g\right\} \\
&= \bigoplus_{g\in G} \frac{R_g}{\sum_{i=1}^{s} R_{gk_i^{-1}} f_i} \ .
\end{aligned}$$

Thus $\left(\frac{R_\bullet}{I}\right)_g = \frac{R_g}{\sum_{i=1}^s R_{gk_i^{-1}} f_i}$. $\square$

Now we have all the machinery in place to prove the following.

Theorem 9. *Let* $K = \frac{\mathbb{F}_p[x_1, \ldots, x_6]}{(x_1^p, \ldots, x_6^p, x_1x_2 + x_3x_4 + x_5x_6)}$ *and* $I = (x_1, \ldots, x_6) \subset K$. *Then* (K, I) *has no divided power structure.*

PROOF. First we endow $R_\bullet = \mathbb{F}_p[x_1 \ldots x_6]$ with a $\mathbb{Z}^3$-grading as follows:

Variable	x_1	x_2	x_3	x_4	x_5	x_6
Degree	$(1,0,0)$	$(-1,0,0)$	$(0,1,0)$	$(0,-1,0)$	$(0,0,1)$	$(0,0,-1)$

Now, $R_{\vec{0}} = \left\{\sum r_{(i,j,k)} x_1^i x_2^i x_3^j x_4^j x_5^k x_6^k : r_{(i,j,k)} \in \mathbb{F}_p\right\}$ and

$$R_{(n,0,0)} = \begin{cases} R_{\vec{0}} x_1^n & n \geq 0 \\ R_{\vec{0}} x_2^{-n} & n < 0 \end{cases},$$

Take a ring A_0 over $\mathbb{F}_p$ with I_0 an ideal of A_0 such that $A_0 = \mathbb{F}_p \oplus I_0$ and $(I_0)^2 = 0$. That is, $\forall x, y \in I_0, xy = 0$. $\square$

Example 10. Let $\mathcal{L} : I_0 \to I_0$, be a (non-zero) linear map. There is a DP structure on (A_0, I_0), constructed as follows:

For all $x \in I_0$ set

$$\begin{aligned} \gamma_0(x) &= 1 , \\ \gamma_1(x) &= x , \\ \gamma_{p^m}(x) &= \mathcal{L}^m(x) , \end{aligned}$$

and for k, not a power of p,

$$\gamma_k(x) = 0 .$$

PROOF.

$$R_{(0,n,0)} = \begin{cases} R_{\vec{0}} x_3^n & n \geq 0 \\ R_{\vec{0}} x_4^{-n} & n < 0 \end{cases},$$

$$R_{(0,0,n)} = \begin{cases} R_{\vec{0}} x_5^n & n \geq 0 \\ R_{\vec{0}} x_6^{-n} & n < 0 \end{cases}.$$

By lemma 8

$$\begin{aligned}\left(\frac{R_\bullet}{(x_1^p,\ldots,x_6^p)}\right)_{\vec{0}} &= \frac{R_{\vec{0}}}{R_{(-p,0,0)}x_1^p + R_{(p,0,0)}x_2^p + R_{(0,-p,0)}x_3^p + R_{(0,p,0)}x_4^p + R_{(0,0,-p)}x_5^p + R_{(0,0,p)}x_6^p} \\ &= \frac{R_{\vec{0}}}{R_{\vec{0}}x_2^p x_1^p + R_{\vec{0}}x_1^p x_2^p + R_{\vec{0}}x_4^p x_3^p + R_{\vec{0}}x_3^p x_4^p + R_{\vec{0}}x_6^p x_5^p + R_{\vec{0}}x_5^p x_6^p} \\ &= \frac{R_{\vec{0}}}{R_{\vec{0}}x_1^p x_2^p + R_{\vec{0}}x_3^p x_4^p + R_{\vec{0}}x_5^p x_6^p}\ .\end{aligned}$$

Now we can see $\dfrac{\mathbb{F}_p[a,b,c]}{(a^p,b^p,c^p)} \simeq \left(\frac{R_\bullet}{(x_1^p,\ldots,x_6^p)}\right)_{\vec{0}}$. Call this isomorphism ϕ. So we have

$$\phi(a) = x_1x_2, \phi(b) = x_3x_4, \phi(c) = x_5x_6\ .$$

For the sake of simpler notation let us define $A_\bullet = \frac{R_\bullet}{(x_1^p,\ldots,x_6^p)}$.

Let

$$f = \phi(a+b+c) = x_1x_2 + x_3x_4 + x_5x_6 \in A_{\vec{0}}\ .$$

Now we have $\frac{A_\bullet}{(f)} = K$. So we can now have a grading on K.

By lemma 7

$$\begin{aligned}K_{\vec{0}} &= \left(\frac{A_\bullet}{(f)}\right)_{\vec{0}} \\ &= \frac{A_{\vec{0}}}{A_{\vec{0}}f} \\ &= \frac{\mathbb{F}_p[a,b,c]}{(a^p,b^p,c^p,a+b+c)} \\ &= \frac{\mathbb{F}_p[b,c]}{(b^p,c^p)}\ .\end{aligned}$$

So say $\omega : \dfrac{\mathbb{F}_p[b,c]}{(b^p,c^p)} \to K_{\vec{0}}$ is the isomorphism with $\omega(b) = x_3x_4$ and $\omega(c) = x_5x_6$.

Now,

$$\omega\left(\sum_{i=1}^{p-1}\frac{(-1)^i(b)^i(c)^{p-i}}{i}\right) = \sum_{i=1}^{p-1}\frac{(-1)^i(x_3x_4)^i(x_5x_6)^{p-i}}{i} = \gamma_p(x_3x_4 + x_5x_6)\ .$$

Over $\mathbb{F}_p$, we know $\dfrac{\mathbb{F}_p[b,c]}{(b^p,c^p)}$ has a basis $\{b^ic^j | i,j < p\}$. Since

$$\sum_{i=1}^{p-1}\frac{(-1)^ib^ic^{p-i}}{i}$$

is a non-zero linear combination of basis elements it is not zero in $\dfrac{\mathbb{F}_p[b,c]}{(b^p,c^p)}$, thus

$$\omega\left(\sum_{i=1}^{p-1}\frac{(-1)^i b^i c^{p-i}}{i}\right)=\gamma_p(x_3x_4+x_5x_6)$$

is not zero in K. But according to the rules of divided powers,

$$\gamma_p(x_3x_4+x_5x_6)=\gamma_p(-x_1x_2)=0\ .$$

So we have the contradiction we have searched for, showing that (K,I) does not have a DP structure. $\square$

CHAPTER 3

Generalizing to Super Rings.

As already mentioned, a super ring R is a $\dfrac{\mathbb{Z}}{2\mathbb{Z}}$-graded ring with homogenous elements in R_0 commuting with everything and homogenous elements of R_1 anti-commuting. That is, for $\xi_i, \xi_j \in R_1$ we have $\xi_i\xi_j = -\xi_j\xi_i$ and for $x \in R_0$ and $y \in R$ we have $xy = yx$. (It is traditional to denote elements in R_1 with ξ's.) Note that anti-commutativity implies that for any ξ in R_1 we have $\xi^2 = 0$. What is the use of super rings in the context of divided powers? As an example, remember that $(\mathbb{Z}[x_i], (x_i))$ has no divided power structure. It happens that $(\mathbb{Z}[\xi_i], (\xi_i))$ does (more technically if $R = \mathbb{Z}[\xi_i]$ then (R_0, R_1R_1) has a divided power structure) **[17]**. A natural question then arises: is it the case that for any super ring A we have a divided power structure on (A_0, A_1A_1)? To study this question it is necessary to fully define what a divided power structure is on a super ring.

3.1. Super Divided Power Structures

Definition 11. Given a super ring $R = R_0 \oplus R_1$ and an ideal $I = I_0 \oplus I_1$ a *super divided power structure* can be defined as follows.

We start with a traditional DP structure on the even part of the ideal, with one extra rule (6) to explain how the super structure interacts with the divided power maps.

(1) $\forall x \in I_0, \gamma_0(x) = 1, \gamma_1(x) = x, \gamma_i(x) \in I_0$ if $i \geq 1$
(2) $\forall x, y \in I_0, \gamma_k(x+y) = \displaystyle\sum_{i+j=k} \gamma_i(x)\gamma_j(y)$
(3) $\forall \lambda \in R_0, \forall x \in I_0, \gamma_k(\lambda x) = \lambda^k \gamma_k(x)$
(4) $\forall x \in I_0, \gamma_i(x)\gamma_j(x) = \frac{(i+j)!}{(i)!(j)!}\gamma_{i+j}(x)$
(5) $\forall x \in I_0, \gamma_p(\gamma_q(x)) = \frac{(pq)!}{p!(q!)^p}\gamma_{pq}(x)$
(6) $\forall \xi_1, \xi_2 \in I_1, \forall k > 1, \gamma_k(\xi_1\xi_2) = 0$

We are not the first to define a "super-rule" like this. When Henri Cartan first presented DP structures he included a similar rule for differential graded algebras.

> "Pour $k \geq 2, \gamma_k(xy) = 0$ si $\deg(x)$ et $\deg(y)$ impairs."**[4]**

This is essentially what we have for (6).

One might expect that given a DP structure on the even part of a ring, that would necessarily give rise to a super DP structure. It turns out that this is not the case.

Example 12. Take a ring A_0 over $\mathbb{F}_p$ with I_0 an ideal of A_0 such that $A_0 = \mathbb{F}_p \oplus I_0$ and $(I_0)^2 = 0$. That is, $\forall x, y \in I_0, xy = 0$.

Let $\mathcal{L} : I_0 \to I_0$, be a (non-zero) linear map. There is a DP structure on (A_0, I_0), constructed as follows:

For all $x \in I_0$ set

$$\begin{aligned} \gamma_0(x) &= 1 \ , \\ \gamma_1(x) &= x \ , \\ \gamma_{p^m}(x) &= \mathcal{L}^m(x) \ , \end{aligned}$$

and for k, not a power of p,

$$\gamma_k(x) = 0 \ .$$

If this is indeed a DP structure (which we will prove in a moment) it cannot be extended to a super DP structure. That is, if we consider it as a divided power structure on (A_0, I_0) for some (non-trivial) super ring $A = A_0 \oplus A_1$, then it does not follow the "super rule[1]". We know that the ideal $A_1A_1 \subset I_0$ since $A_0 = \mathbb{F}_p \oplus I_0$ so if there is a DP structure the super rule should apply on the elements of A_1A_1. However $\gamma_p(\xi_1\xi_2) = \mathcal{L}(\xi_1\xi_2)$, which is not zero, so the super rule is not in effect.

Claim 13. Example 12 does in fact define a DP structure.

PROOF. To prove it is a DP structure we must prove that each of the five rules are satisfied. *Rule 1* is satisfied directly by the definition.

We will start with *Rule 3*.

Let $\lambda \in A_0, x \in I_0$. For k, not a power of p, we have

$$\gamma_k(\lambda x) = 0 = \lambda^k \cdot 0 = \lambda^k \gamma_k(x)$$

and for powers of p, we can say $\lambda = c + i$ where $c \in \mathbb{F}_p, i \in I_0$, so

$$\gamma_{p^m}(\lambda x) = \mathcal{L}^m(cx + ix) = \mathcal{L}^m(cx) = c\mathcal{L}^m(x) = c^{p^m}\mathcal{L}^m(x) = \lambda^{p^m}\gamma_{p^m}(x)$$

So *Rule 3* is satisfied[2].

[1]Rule 6, $\forall \xi_1, \xi_2 \in I_1, \forall k > 1, \gamma_k(\xi_1\xi_2) = 0$

[2]We have $c^{p^m} \equiv_p c$ by Fermat's Little Theorem.

Now for *Rule 2*.

Let $x, y \in I_0$.

First we can simplify things a bit,

$$\sum_{i=0}^{k} \gamma_i(x)\gamma_{k-i}(y) = \gamma_k(x) + \gamma_k(y)$$

since $(I_0)^2 = 0$.

For k, not a power of p, we have

$$\gamma_k(x) + \gamma_k(y) = 0 + 0 = 0 = \gamma_k(x+y)$$

and for a power of p we have

$$\gamma_{p^m}(x) + \gamma_{p^m}(y) = \mathcal{L}^m(x) + \mathcal{L}^m(y) = \mathcal{L}^m(x+y) = \gamma_{p^m}(x+y) \ .$$

Thus *Rule 2* is satisfied.

On to *Rule 4*.

Let $x \in I_0$. For k not a power of p, and $i \in \mathbb{N}$ we have

$$\gamma_i(x)\gamma_{k-i}(x) = 0 = \binom{k}{i} \cdot 0 = \binom{k}{i}\gamma_k(x) \ .$$

For a power of p, $\binom{p^m}{i}$ is divisible by p so

$$\gamma_i(x)\gamma_{p^m-i}(x) = 0 = 0 \cdot \gamma_{p^m}(x) = \binom{p^m}{i}\gamma_{p^m}(x) \ .$$

Now *Rule 4* is satisfied.

Lastly *Rule 5*.

Let $x \in I_0$. If at least one of q or r is not a power of p, then

$$\gamma_q(\gamma_r(x)) = 0 = \frac{(qr)!}{q!(r!)^q} \cdot 0 = \frac{(qr)!}{q!(r!)^q}\gamma_{qr}(x)$$

If $q = p^s$ and $r = p^t$ we know $\frac{p^{s+t}!}{p^s!(p^t!)^{p^s}} \equiv_p 1$ (see A.2), so then

$$\gamma_{p^s}(\gamma_{p^t}(x)) = \gamma_{p^s}(\mathcal{L}^t(x)) = \mathcal{L}^{s+t}(x) = \frac{p^{s+t}!}{p^s!(p^t!)^{p^s}}\mathcal{L}^{s+t}(x) = \frac{p^{s+t}!}{p^s!(p^t!)^{p^s}}\gamma_{p^{s+t}}(x)$$

Therefore, *rule 5* is satisfied and this is a PD structure. $\square$

CHAPTER 4

The Koblitz Example sits in a Super Ring.

To prove that the Koblitz Example is a subring of a super ring, we will prove a more general result. Any ring of the form $\dfrac{\mathbb{F}_p[x_1, \ldots, x_n]}{\left(x_1^{k_1}, \ldots, x_n^{k_n}, t\right)}$, where $2 \leq k_1, \ldots, k_n \leq p$ and $t \in \mathbb{F}_p[x_1, \ldots, x_n]$, is isomorphic to a subring of some super ring. The key here is recognizing that any nilpotent element can be constructed as a sum of square-zero elements. For example if x and y are nilpotent elements of some ring with $x^2 = 0$ and $y^2 = 0$, then $(x+y)^2 = xy$ and $(x+y)^3 = 0$. Using that idea we can inject the Koblitz ring into a ring with square-zero generators[1], which can itself be injected into a super ring.

Theorem 14. *For any $k \leq p$ we have an injection of $\dfrac{\mathbb{F}_p[x]}{(x^k)}$ into $\dfrac{\mathbb{F}_p[x_1, \ldots, x_{k-1}]}{(x_i^2)}$.*

Proof. Define a homomorphism $\varphi : \dfrac{\mathbb{F}_p[x]}{(x^k)} \to \dfrac{\mathbb{F}_p[x_1, \ldots, x_{k-1}]}{(x_i^2)}$ by $\varphi(x) = \displaystyle\sum_{i=1}^{k-1} x_j$. This is well defined because by the multinomial theorem

$$\left(\sum_{i=1}^{k-1} x_i\right)^k = \sum_{j_1+j_2+\cdots+j_{k-1}=k} \binom{n}{j_1, j_2, \ldots, j_{k-1}} \prod_{1 \leq t \leq k-1} x_t^{j_t}$$

and by the pigeon hole principle for each summand there must be at least one $j_t \geq 2$ which means each summand is 0. Thus $\left(\displaystyle\sum_{i=1}^{k-1} x_i\right)^k = 0$, and φ is well defined. Suppose $r \in \ker \varphi$. Since $r \in \dfrac{\mathbb{F}_p[x]}{(x^k)}$ it can be written uniquely as $\displaystyle\sum_{h=0}^{k-1} c_h x^h$ where $\forall h, c_h \in \mathbb{F}_p$.

[1]There is a fun representation of rings of this type that we will discuss in Appendix B.

Now we have $\sum_{h=0}^{k-1} c_h x^h \in \ker\varphi$ and we can calculate,

$$\begin{aligned}
\varphi\left(\sum_{h=0}^{k-1} c_h x^h\right) &= \sum_{h=0}^{k-1} c_h \left(\varphi(x)\right)^h \\
&= \sum_{h=0}^{k-1} c_h \left(\sum_{j=1}^{k-1} x_j\right)^h \\
&= \sum_{h=0}^{k-1} c_h \left(\sum_{|M|=h} (h!) \prod_{j\in M} x_j\right) \\
&= \sum_{h=0}^{k-1} \sum_{|M|=h} (h!)\, c_h \prod_{j\in M} x_j
\end{aligned}$$

where each M in the summation is a subset of $\{1,\ldots,k-1\}$. Now

$$\left\{\prod_{j\in M} x_j \mid M \subset \{1,\ldots,k-1\}\right\}$$

is a linearly independent set and

$$\sum_{h=0}^{k-1}\sum_{|M|=h} (h!)\, c_h \prod_{j\in M} x_j = 0 \ .$$

Thus, $\forall h, (h!)\, c_h = 0$, and since h is less than p, $h!$ is non-zero, so that means $c_h = 0$ for every h. Therefore $\sum_{h=0}^{k-1} c_h x^h = r = 0$, so $\ker\varphi = \{0\}$, thus φ is injective. ☐

Now we are going to show $\dfrac{\mathbb{F}_p[x]}{(x^k)} \simeq \left(\dfrac{\mathbb{F}_p[x_1,\ldots,x_{k-1}]}{(x_i^2)}\right)^{S_{k-1}}$ but we require some more tools first.[2]

Lemma 15. *For any G-modules M and N, we have $(M\oplus N)^G = M^G \oplus N^G$.*

Proof. Let $(m,n) \in (M\oplus N)^G$, and $g \in G$. Then we have

$$(m,n) = g\cdot(m,n) = (g\cdot m, g\cdot n)$$

So $m = g\cdot m$ and $n = g\cdot n$, thus $m\oplus n \in M^G \oplus N^G$. Which means $(M\oplus N)^G \subset M^G\oplus N^G$, and note that the same calculation read backwards also shows that $M^G \oplus N^G \subset (M\oplus N)^G$, so $(M\oplus N)^G = M^G\oplus N^G$. Thus, invariance under a group action commutes with direct sums. ☐

[2]These tools are well known. We include them for the sake of completeness.

Theorem 16. *If $k \le p$, then $\dfrac{\mathbb{F}_p[x]}{(x^k)}$ is isomorphic to $\left(\dfrac{\mathbb{F}_p[x_1,\dots,x_{k-1}]}{(x_i^2)}\right)^{S_{k-1}}$.*

Proof. For the sake of easier notation say $R = \dfrac{\mathbb{F}_p[x]}{(x^k)}$ and $A = \dfrac{\mathbb{F}_p[x_1,\dots,x_{k-1}]}{(x_i^2)}$. Since $\varphi : R \to A$ is injective we know that $R \simeq \varphi(R)$, so it suffices to show that $\varphi(R) = A^{S_{k-1}}$.

We have $\varphi(R)$ and $A^{S_{k-1}}$ are both subrings of A, and we know $\varphi(R)$ is generated by $\displaystyle\sum_{j=1}^{k-1} x_j$ which is in $A^{S_{k-1}}$, so $\varphi(R) \subset A^{S_{k-1}}$.

Now to show $A^{S_{k-1}} \subset \varphi(R)$. Observe that $R = \bigoplus_{h=0}^{k-1} R_h$ has dimension k. Also note that since invariance under a module preserving group action commutes with direct sums by Lemma 15, and S_{k-1} preserves the degree of the monomials it acts upon so we have

$$A^{S_{k-1}} = \left(\bigoplus_{h=0}^{k-1} A_h\right)^{S_{k-1}} = \bigoplus_{h=0}^{k-1} (A_h)^{S_{k-1}} = \bigoplus_{h=0}^{k-1} \left(A^{S_{k-1}}\right)_h .$$

and each $\left(A^{S_{k-1}}\right)_h$ is generated by only one generator $\displaystyle\sum_{|M|=h}\prod_{j\in M} x_j$. Thus each $\left(A^{S_{k-1}}\right)_h$ is one dimensional. So the total dimension of $A^{S_{k-1}}$ is k. Since φ is an injection and $\dim(R) = k$, the dimension of $\varphi(R) = k$ as well, which implies $\varphi(R) = A^{S_{k-1}}$.

Thus, $A^{S_{k-1}} = \varphi(R)$. Which means, since φ is injective, that $R \simeq A^{S_{k-1}}$, that is to say $\dfrac{\mathbb{F}_p[x]}{(x^k)} \simeq \left(\dfrac{\mathbb{F}_p[x_1,\dots,x_{k-1}]}{(x_i^2)}\right)^{S_{k-1}}$. □

Remember our goal is to show a result about rings of the form $\dfrac{\mathbb{F}_p[x_1,\dots,x_n]}{\left(x_1^{k_1},\dots,x_n^{k_n},t\right)}$. So far we have a result for rings of the form $\dfrac{\mathbb{F}_p[x]}{(x^k)}$. We will extend this to rings of the form $\dfrac{\mathbb{F}_p[x_1,\dots,x_n]}{\left(x_1^{k_1},\dots,x_n^{k_n}\right)}$ by recognizing that they are just tensor products of n rings with one variable; and since each $\dfrac{\mathbb{F}_p[x]}{(x^k)}$ is a finitely generated free $\mathbb{F}_p$-module tensoring them over $\mathbb{F}_p$ is exact.

Lemma 17. *Given two $\mathbb{F}_p$-vector spaces V and W and two groups, G and H, where G acts on V and H acts on W, then $V^G \otimes W^H = (V \otimes W)^{G\times H}$, and $G \times H$ acts on $(V \otimes W)$ by $(g,h)\cdot(v\otimes w) = (g\cdot v \otimes h\cdot w)$. (So long as $|G|$ and $|H|$ are non-zero in $\mathbb{F}_p$.)*

PROOF. Let $\sum_i(v_i \otimes w_i) \in V^G \otimes W^H$, let $(g,h) \in G \times H$. Now,

$$(g,h) \cdot \sum_i (v_i \otimes w_i) = \sum_i (g \cdot v_i \otimes h \cdot w_i) = \sum_i (v_i \otimes w_i) \ .$$

So $V^G \otimes W^H \subset (V \otimes W)^{G \times H}$.

Let $\sum_i(v_i \otimes w_i) \in (V \otimes W)^{G\times H}$, we want to show that for each i there is $v'_i \in V^G$ and $w'_i \in W^H$ such that $(v'_i \otimes w'_i) = (v_i \otimes w_i)$. For every i put $v'_i = \frac{1}{|G|}\sum_{g\in G} g \cdot v_i$, and $w'_i = \frac{1}{|H|}\sum_{h \in H} h \cdot w_i$.

Now let $f \in G$, for each i

$$\begin{aligned} f \cdot v'_i &= f \cdot \left(\frac{1}{|G|} \sum_{g\in G} g \cdot v_i \right) \\ &= \frac{1}{|G|} \sum_{g \in G} fg \cdot v_i \\ &= \frac{1}{|G|} \sum_{g\in G} g \cdot v_i \\ &= v'_i \end{aligned} \tag{4.0.1}$$

So each $v'_i \in V^G$ and by a similar demonstration each $w'_i \in W^H$.

Now,

$$\begin{aligned} \sum_i (v'_i \otimes w'_i) &= \sum_i \left(\frac{1}{|G|}\sum_{g\in G} g \cdot v_i \otimes \frac{1}{|H|} \sum_{h\in H} h \cdot w_i \right) \\ &= \sum_i \frac{1}{|G|\,|H|} \sum_{g\in G} \sum_{h \in H} (g \cdot v_i \otimes h \cdot w_i) \\ &= \sum_i \frac{1}{|G|\,|H|} \sum_{g\in G} \sum_{h \in H} (g,h) \cdot (v_i \otimes w_i) \\ &= \frac{1}{|G|\,|H|} \sum_{g\in G} \sum_{h \in H} (g,h) \sum_i (v_i \otimes w_i) \\ &= \frac{1}{|G|\,|H|} \sum_{g\in G} \sum_{h \in H} \sum_i (v_i \otimes w_i) \\ &= \sum_i (v_i \otimes w_i) \end{aligned}$$

Thus $\sum_i(v_i \otimes w_i) = \sum_i(v'_i \otimes w'_i) \in V^G \otimes_R W^H$ so $(V \otimes_R W)^{G\times H} \subset V^G \otimes_R W^H$. Which means $V^G \otimes_R W^H = (V \otimes_R W)^{G \times H}$ as required. $\square$

In our situation if

$$R = \frac{\mathbb{F}_p\left[x_1, x_2\right]}{\left(x_1^{k_1}, x_2^{k_2}\right)} = \frac{\mathbb{F}_p\left[x_1\right]}{\left(x_1^{k_1}\right)} \otimes \frac{\mathbb{F}_p\left[x_2\right]}{\left(x_2^{k_2}\right)}$$

and

$$\begin{aligned} A &= \frac{\mathbb{F}_p\left[x_{(1,1)}, \ldots, x_{(1,k_1-1)}, x_{(2,1)}, \ldots, x_{(2,k_2-1)}\right]}{\left(x_{(i,j)}^2\right)} \\ &= \frac{\mathbb{F}_p\left[x_1, \ldots, x_{k_1-1}\right]}{\left(x_i^2\right)} \otimes \frac{\mathbb{F}_p\left[x_1, \ldots, x_{k_2-1}\right]}{\left(x_i^2\right)} \end{aligned}$$

then lemma 17 says that

$$\begin{aligned} A^{S_{k_1-1}\times S_{k_2-1}} &= \left(\frac{\mathbb{F}_p[x_{(1,1)}, \ldots, x_{(1,k_1-1)}, x_{(2,1)}, \ldots, x_{(2,k_2-1)}]}{(x_{(i,j)}^2)}\right)^{S_{k_1-1}\times S_{k_2-1}} \\ &= \left(\frac{\mathbb{F}_p\left[x_1, \ldots, x_{k_1-1}\right]}{(x_i^2)}\right)^{S_{k_1-1}} \otimes \left(\frac{\mathbb{F}_p\left[x_1, \ldots, x_{k_2-1}\right]}{(x_i^2)}\right)^{S_{k_2-1}} \\ &= \frac{\mathbb{F}_p\left[x_1\right]}{\left(x_1^{k_1}\right)} \otimes \frac{\mathbb{F}_p\left[x_2\right]}{\left(x_2^{k_2}\right)} \\ &= \frac{\mathbb{F}_p\left[x_1, x_2\right]}{\left(x_1^{k_1}, x_2^{k_2}\right)} \\ &= R \end{aligned}$$

which is what we need. By induction this can be extended to any finite number of variables.

Now we want to bring the t of $\dfrac{\mathbb{F}_p[x_1, \ldots, x_n]}{\left(x_1^{k_1}, \ldots, x_n^{k_n}, t\right)}$ into the picture.

Lemma 18. *Let R and A be rings. Let G be a group acting on A with $|G|$ invertible in both R and A. Let $\phi : R \to A$, be an injection of R into A, such that $\phi(R) = A^G$. Then $\forall t \in R$ there is an injection of $\frac{R}{(t)}$ into $\frac{A}{(\phi(t))}$.*

Proof. Let $t \in R$, we want to show that $\psi : \frac{R}{(t)} \to \frac{A}{(\phi(t))}$ with $\psi\left(r + (t)\right) = \phi(r) + (\phi(t))$, is an injection.

Let $r + (t) \in \ker\psi$. For the sake of simplicity set $s = \phi(t)$. Now $\phi(r) \in (s)$. So $\phi(r) = \alpha s$, for some $\alpha \in A$.

Define $\beta = \frac{1}{|G|}\sum_{g\in G} g \cdot \alpha$. Note: we are able to divide by $|G|$ since it is invertible.

Let $f \in G$. Now by the same calculations as 4.0.1 on the preceding page we have $f \cdot \beta = \beta$, so we know $\beta \in A^G = \phi(R)$.

Now $\beta s = \frac{1}{|G|}\sum_{g\in G}(g\cdot\alpha)s$, but $(g\cdot\alpha)s = (g\cdot\alpha)(g\cdot s) = g\cdot(\alpha s) = \alpha s$ since $\alpha s \in \phi(R) = A^G$. Thus,

$$\begin{aligned}\beta s &= \frac{1}{|G|}\sum_{g\in G}(g\cdot\alpha)s\\ &= \frac{1}{|G|}\sum_{g\in G}\alpha s\\ &= \alpha s\end{aligned}$$

so $\phi(r) = \beta s$. Pick $b \in R$ such that $\phi(b) = \beta$. Now $\phi(r) = \phi(b)\phi(t) = \phi(bt)$. Since ϕ is injective, we have $r \in (t)$.

So we have just shown if $\phi(r) \in (\phi(t)) \subset A$, then $r \in (t)$. Now $\psi(r + (t)) = 0$ implies that $\phi(r) \in (\phi(t))$, which implies that $r \in (t)$, that is $r + (t) = 0$. So $\ker\psi = \{0\}$, and ψ is injective. $\square$

Applying this lemma 18 to our case, the only thing we need to check is if $|\prod_{i=1}^n S_{k_i-1}| = \prod_{i=1}^n\big((k_i-1)!\big)$ is invertible, which it is since it has no p factors. Thus, if

$$R = \frac{\mathbb{F}_p[x_1,\ldots,x_n]}{\left(x_1^{k_1},\ldots,x_n^{k_n}\right)},$$

$$A = \frac{\mathbb{F}_p[x_{(1,1)},\ldots,x_{(1,k_1-1)},\ldots,x_{(n,1)},\ldots x_{(n,k_n-1)}]}{\left(x_{(i,j)}^2\right)},$$

and $t \in R$, then we know from lemma 17 that there is an injective homomorphism $\varphi : R \hookrightarrow A$ and from lemma 18 we know that $\dfrac{R}{(t)}$ is isomorphic to a subring of $\dfrac{A}{(\varphi(t))}$.

Now we simply need to show rings like A can be injected into super rings.

Lemma 19. *If $B = \dfrac{\mathbb{F}_p[y_1,\ldots,y_m]}{(y_i^2)}$, then there is a super-ring SR with a subring isomorphic to B. Specifically the group $G = \left(\frac{\mathbb{Z}}{2\mathbb{Z}}\right)^m$ acts on SR and $B \cong (SR)^G$*

Proof. Let $SR = \mathbb{F}_p[\xi_1,\ldots,\xi_{2m}]$, where each ξ_i is an anti-commutative variable. Remember the ξ_i's have the property that $\xi_i^2 = 0$ so the only exponents that exist are 0 and 1.

The group $G = \left(\frac{\mathbb{Z}}{2\mathbb{Z}}\right)^m$ acts on SR with $(0,\ldots,1,\ldots,0)$ (one in the j^{th} place) sending $\xi_{2j-1} \mapsto -\xi_{2j-1}$ and $\xi_{2j} \mapsto -\xi_{2j}$.

So now $(SR)^G = \left\{\sum_{\vec{k}\in\left(\frac{\mathbb{Z}}{2\mathbb{Z}}\right)^m} c_{\vec{k}}\xi_1^{k_1}\xi_2^{k_1}\cdots\xi_{2m-1}^{k_m}\xi_{2m}^{k_m} \mid \forall\vec{k}, c_{\vec{k}} \in \mathbb{F}_p\right\} \simeq B$. Which completes the proof. $\square$

Now, each ring A, that we were speaking of earlier in 4, has similar structure to B, and so for each A there is a super-ring SR that has a subring isomorphic to it. Thus there is an injection $\omega : A \to SR$, with $\omega(A) = (SR)^G$, and by lemma 18, $\forall s \in A$, $\frac{A}{(s)}$ injects into $\frac{SR}{(\omega(s))}$.

Now with regards to the Koblitz Example. Define:

$$K = \frac{\mathbb{F}_p[x_1, \ldots, x_6]}{(x_1^p, \ldots, x_6^p, x_1x_2 + x_3x_4 + x_5x_6)} .$$

Theorem 20. *There exist super rings $A = A_0 \oplus A_1$ without any divided power structure on (A_0, A_1A_1). Specifically, K is isomorphic to a subring of a super ring SR, and since $(K, (x_i))$ has no DP structure, neither does (SR_0, SR_1SR_1).*

Proof. We have shown that there exists an injection φ taking K into a ring of the form

$$A = \frac{\mathbb{F}_p[x_{(1,1)}, \ldots, x_{(1,p-1)}, \ldots, x_{(6,1)}, \ldots x_{(6,p-1)}]}{\left(x_{(1,1)}^2, \ldots, x_{(6,p-1)}^2, \varphi\left(x_1x_2 + x_3x_4 + x_5x_6\right)\right)} .$$

We have also shown the existence of an injection ω taking A into a super ring

$$SR = \frac{\mathbb{F}_p[\xi_1, \ldots, \xi_{12(p-1)}]}{(\omega \circ \varphi\left(x_1x_2 + x_3x_4 + x_5x_6\right))} .$$

By our construction $\omega \circ \varphi((x_i)) \subset SR_1SR_1$, so if (SR_0, SR_1SR_1) did have a divided structure γ it would have the same issues as the Koblitz example creating a contradiction. Which means that (SR_0, SR_1SR_1) has no divided power structure. $\square$

APPENDIX A

Some Calculations

A.1. On factorials mod p.

Fact 21. *For $i < p$, $i!(p-i)! \equiv_p (-1)^i\, i$.*

PROOF. Wilson's theorem says for prime p, we have $1!\,(p-1)! \equiv_p (-1)^1\, 1$. If $k!(p-k)! \equiv_p (-1)^k\, k$ then we calculate,

$$\begin{aligned}(k+1)!(p-k-1)! &= \frac{(k+1)}{(p-k)} k!(p-k)! \\ &\equiv_p \frac{(k+1)}{(p-k)} (-1)^k\, k \\ &= (-1)^{k+1} (k+1) \frac{k}{k-p} \\ &\equiv_p (-1)^{k+1} (k+1)\ .\end{aligned}$$

So we have the result by induction. $\square$

A.2. Showing that $\dfrac{p^{s+t}!}{p^s!(p^t!)^{p^s}}$ is congruent to 1 modulo p.

In order to prove this we need to first prove a lemma.

The well known formula for the first (non-zero) digit from the right of $n!$ in base-p is

$$(-1)^{\mathrm{ord}_p(n!)}(\prod_{i=0}^{r} n_i!)$$

modulo p. (Where n_i is the i^{th} digit of n in base p.) **[14]**

Lemma 22. *In the case of $n = p^r$ the formula reduces to $(-1)^{\frac{p^r-1}{p-1}}$ modulo p.*

PROOF. Given a finite set of natural numbers M define $M!$ to be $\prod_{m\in M} m$, the product of all of the numbers in M, (of course $\emptyset! = 1$). Define $\mu(M)$ to be the first (non-zero) digit of $M!$ in base-p. So now the task is to determine that $\mu(\{1,\ldots,p^r\}) \equiv_p (-1)^{\frac{p^r-1}{p-1}}$. We see that if A and B are disjoint subsets of $\mathbb{N}$, then $(A \sqcup B)! = A!B!$. Thus, $\mu(A \sqcup B) \equiv_p \mu(A)\mu(B)$.

Now $\{1,\ldots,p^r\}$ can be partitioned into $A_0 \sqcup \ldots \sqcup A_r$ by defining each A_i like so: $A_i = \{m \in \{1,\ldots,p^r\} | \mathrm{ord}_p(m) = i\}$. Now for $i < r$, $\mu(A_i) \equiv_p (p-1)!^{p^{r-i-1}} \equiv_p$

$(-1)^{p^{r-i-1}}$, since for each possible first digit $m_i \in \{1, \ldots, p-1\}$ there are p^{r-i-1} possibilities for the higher digits. ($(p-1)! \equiv_p (-1)$ by Wilson's Theorem.) And of course $\mu(A_r) = 1$.

So

$$\begin{aligned}\mu(\{1, \ldots, p^r\}) &\equiv_p \prod_{i=0}^{r} \mu(A_i) \\ &\equiv_p (-1)^{\sum_{i=0}^{r} p^{r-i-1}} \\ &\equiv_p (-1)^{\frac{p^r-1}{p-1}}\end{aligned}$$

Thus $(p^r)! \equiv_p (-1)^{\frac{p^r-1}{p-1}}$. □

Fact. *It is the case that* $\frac{p^{s+t}!}{p^s!(p^t!)^{p^s}} \equiv_p 1$.

PROOF. Note: for any odd prime p, $\frac{p^t-1}{p-1}$ has the same parity as t. (Induction on t using $\dfrac{p^t-1}{p-1} = \displaystyle\sum_{i=0}^{t-1} p^i$.)

From the above formula we know the first digit of $p^{s+t}!$ is $(-1)^{\frac{p^{s+t}-1}{p-1}} \equiv_p (-1)^{s+t}$, the first digit of $p^s!$ is $(-1)^{\frac{p^s-1}{p-1}} \equiv_p (-1)^s$, and the first digit of $p^t!$ is $(-1)^{\frac{p^t-1}{p-1}} \equiv_p (-1)^t$. So for odd p, the first digit of $p^s!(p^t!)^{p^s}$ is $(-1)^s(-1)^{tp^s} \equiv_p (-1)^{s+t}$ (since p^s is odd). Thus the first digit of $\dfrac{p^{s+t}!}{p^s!(p^t!)^{p^s}}$ is $\dfrac{(-1)^{s+t}}{(-1)^{s+t}} = 1$, as we'd hoped. (When $p = 2$, knowing that p does not divide $\dfrac{p^{s+t}!}{p^s!(p^t!)^{p^s}}$ is enough to know that the first digit is not zero, so it must be one.)

Now we have the required result. □

APPENDIX B

A Fun Representation of Rings With Square-Zero Generators.

The following is just for fun.

Elements $a + bx$ of a ring $\dfrac{k[x]}{(x^2)}$ can be represented by a matrix $\begin{bmatrix} a & b \\ 0 & a \end{bmatrix}$. To increase the number of variables we can take the Kronecker product $\otimes$ of two matrices representing $a + bx \in \dfrac{k[x]}{(x^2)}$ and $c + dy \in \dfrac{k[y]}{(y^2)}$:

$$\begin{bmatrix} a & b \\ 0 & a \end{bmatrix} \otimes \begin{bmatrix} c & d \\ 0 & c \end{bmatrix} = \begin{bmatrix} ac & ad & bc & bd \\ 0 & ac & 0 & bc \\ 0 & 0 & ac & ad \\ 0 & 0 & 0 & ac \end{bmatrix} .$$

So a general element $a + bx + cy + dxy$ of $\dfrac{k[x,y]}{(x^2, y^2)}$ can be represented as:

$$\begin{bmatrix} a & c & b & d \\ 0 & a & 0 & b \\ 0 & 0 & a & c \\ 0 & 0 & 0 & a \end{bmatrix} .$$

Taking this a few steps further, elements of $\dfrac{k[x_1, \ldots, x_4]}{(x_i^2)}$ can be represented as

$$\begin{bmatrix}
a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & a_7 & a_8 & a_9 & a_{10} & a_{11} & a_{12} & a_{13} & a_{14} & a_{15} & a_{16} \\
 & a_1 & & a_3 & & a_5 & & a_7 & & a_9 & & a_{11} & & a_{13} & & a_{15} \\
 & & a_1 & a_2 & & & a_5 & a_6 & & & a_9 & a_{10} & & & a_{13} & a_{14} \\
 & & & a_1 & & & & a_5 & & & & a_9 & & & & a_{13} \\
 & & & & a_1 & a_2 & a_3 & a_4 & & & & & a_9 & a_{10} & a_{11} & a_{12} \\
 & & & & & a_1 & & a_3 & & & & & & a_9 & & a_{11} \\
 & & & & & & a_1 & a_2 & & & & & & & a_9 & a_{10} \\
 & & & & & & & a_1 & & & & & & & & a_9 \\
 & & & & & & & & a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & a_7 & a_8 \\
 & & & & & & & & & a_1 & & a_3 & & a_5 & & a_7 \\
 & & & & & & & & & & a_1 & a_2 & & & a_5 & a_6 \\
 & & & & & & & & & & & a_1 & & & & a_5 \\
 & & & & & & & & & & & & a_1 & a_2 & a_3 & a_4 \\
 & & & & & & & & & & & & & a_1 & & a_3 \\
 & & & & & & & & & & & & & & a_1 & a_2 \\
 & & & & & & & & & & & & & & & a_1
\end{bmatrix}$$

and $\dfrac{k[x_1, \ldots, x_n]}{(x_i^2)}$ can be represented by $2^n \times 2^n$ matrices with the entries forming the n^{th} iteration of Sierpinski's triangle, and all the entries on a diagonal equal. The fractal is formed since a sheet of paper is a metric space and the Kronecker product naturally forms a iterative function system on it [**6**]. As far as we can tell this has no real uses, save being a Martin Gardner-esque curiosity.

Bibliography

[1] Glenn Barnich, Friedemann Brandt, and Marc Henneaux. Local BRST cohomology in gauge theories. *Physics Reports*, 338(5):439–569, November 2000. 1.5

[2] Pierre Berthelot. Ideaux a puissances divisees. In *Cohomologie Cristalline des Schémas de Caractéristique p>o*, number 407 in Lecture Notes in Mathematics, pages 26–79. Springer Berlin Heidelberg, January 1974. 1.3, 1.4

[3] Pierre Berthelot and Arthur Ogus. *Notes on Crystalline Cohomology.* Princeton University Press, 1978. 1.3, 4, 5, 2

[4] Henri Cartan. Puissances divisées. In *Séminaire Henri Cartan: Algèbre D'Eilenberg - Mac Lane et homotopie.*, volume 7, École Normale Supérieure, Paris, January 1955. 1.4, 3.1

[5] Pierre Deligne. La conjecture de weil. i. *Publications Mathématiques*, 43:273–307, 1973. 1.3

[6] Matthew Demers. Fractal attractors and iterated function systems. Keynote Pesentation at the Southwestern Ontario Graduate Mathematics Conference, June 2013. B

[7] Jean Dieudonné. *A history of algebraic and differential topology, 1900-1960.* Birkhäuser, Boston, 1989. 1.1

[8] David Steven Dummit and Richard M Foote. *Abstract algebra.* Wiley, Hoboken, NJ, 2004. 1.2

[9] Bernard Dwork. On the rationality of the zeta function of an algebraic variety. *American Journal of Mathematics*, 82(3):631, July 1960. 1.3

[10] Alexander Grothendieck. Sur quelques points d'algèbre homologique, i. *Tohoku Mathematical Journal*, 9(2):119–221, 1957. Mathematical Reviews number (MathSciNet) MR0102537. 1.2

[11] Alexander Grothendieck. On the de rham cohomology of algebraic varieties. *Publications mathématiques de l'I.H.É.S.*, 29:95–103, 1966. 1.2

[12] Stephen Hawking. *The universe in a nutshell.* Bantam Books, New York, 2001. 1.6

[13] I. M. James. *History of Topology.* Elsevier, August 1999. 1.1, 1.2

[14] Neal Koblitz. *p-adic Numbers, p-adic Analysis, and Zeta-Functions.* Number 58 in Graduate Texts in Mathematics. Springer-Verlag, second edition, 1984. A.2

[15] Norbert Roby. Lois polynomes et lois formelles en théorie des modules. *Annales Scientifiques de l'École Normale Supérieure. Troisième Série*, 80:213–348, 1963. 1.4

[16] Hans Samelson. Differential forms, the early days; or the stories of deahna's theorem and of volterra's theorem. *The American Mathematical Monthly*, 108(6):522, June 2001. 1.1

[17] A. Schwarz and I. Shapiro. Supergeometry and arithmetic geometry. *Nuclear Physics B*, 756(3):207–218, 2006. 1, 1.7, 3

[18] A. Schwarz and I. Shapiro. p-adic superspaces and frobenius. *Communications in Mathematical Physics*, 282(1):87–113, 2008. 1.1

[19] John Tate. Homology of noetherian rings and local rings. *Illinois Journal of Mathematics*, 1(1):14–27, March 1957. 1.5, 1.5

[20] André Weil. Numbers of solutions of equations in finite fields. *Bulletin of the American Mathematical Society*, 55(5):497–508, 1949. 1.3

Vita Auctoris

Reg Robson was born in Windsor, Ontario in 1987. He graduated from Vincent Massey Secondary School in 2005. He went on to the University of Windsor where he became a leader in the newly re-founded Math and Stats Association. He graduated in 2011 with a Hon. B. Math and a B. Ed. He is currently a candidate for a Masters degree in Mathematics at the University of Windsor and hopes to graduate in the spring of 2014.