Journal of Pure and Applied Algebra 213 (2009) 1290–1298

Contents lists available at ScienceDirect

Journal of Pure and Applied Algebra

journal homepage: www.elsevier.com/locate/jpaa

# On the classifying ring for Abel formal group laws

Francis Clarke [a,*], Keith Johnson [b]

[a] Department of Mathematics, Swansea University, Swansea SA2 8PP, Wales, United Kingdom
[b] Department of Mathematics, Dalhousie University, Halifax, Nova Scotia, Canada B3H 4R2

ARTICLE INFO

*Article history:*
Received 17 June 2008
Received in revised form 29 October 2008
Available online 30 December 2008
Communicated by P. Balmer

*MSC:*
55N22
13F20

ABSTRACT

The ring over which the universal Abel formal group law is defined is characterized by an integrality condition. Three localizations of this ring considered by Bukhshtaber and Kholodov are given simple descriptions in terms of integer-valued polynomials, and the Abel formal group over one of these rings is shown to be multiplicative.

## 1. Introduction

An *Abel formal group law* over a ring $R$ is a formal group law $F(u, v) \in R[[u, v]]$ of the form

$$F(u, v) = u + v + \alpha_1 uv + \sum_{i>1} \alpha_i (uv^i + u^i v). \tag{1.1}$$

It is well known that a complex-oriented cohomology theory has associated to it a formal group law, and Busato showed in [1] that there is a cohomology theory $Ab^*(\quad)$ whose associated formal group law is the universal Abel formal group law $F_{\mathrm{Ab}}$. This result is based on earlier work [2] by Bukhshtaber and Kholodov who constructed the ring $\Lambda$ over which the universal Abel formal group law is defined and which forms the coefficient ring of $Ab^*(\quad)$. They also constructed cohomology theories whose coefficient rings are certain localizations of $\Lambda$ and established certain algebraic facts about $\Lambda$, including that $\Lambda$ is torsion-free and that $\Lambda \otimes \mathbb{Q}$ is isomorphic to the ring $\mathbb{Q}[a, b]^{S_2}$ of symmetric polynomials in the roots $a$ and $b$ of the quadratic $X^2 - \alpha_1 X - 2\alpha_2$. Thus $\Lambda$ may be considered to be a subring of $\mathbb{Q}[a, b]$. Bukhshtaber and Kholodov also described $\Lambda$ in terms of generators and relations, and gave a $\mathbb{Z}_{(p)}$-basis for the localization of $\Lambda$ at a prime $p$; see Propositions 2.3 and 3.3 below.

In this paper, we show that $\Lambda$ can be described by an integrality condition: a polynomial $f(a, b) \in \mathbb{Q}[a, b]^{S_2}$ lies in $\Lambda$ if and only if it has the property that $f(kt, \ell t) \in \mathbb{Z}[t, (k - \ell)^{-1}]$ for any pair of distinct integers $k$ and $\ell$. Using this criterion, we show that the localizations of $\Lambda$ considered in [2] have similar descriptions in terms of integrality conditions and that over one of these localizations $F_{\mathrm{Ab}}$ is isomorphic to the multiplicative formal group law.

The organization of the paper is as follows: Section 2 contains a summary of the facts we need from [1,2] about Abel formal group laws and the statement of our main result, Theorem 2.4. Its proof, in Section 3, consists in showing that (i) the elements of $\Lambda$ satisfy the integrality condition (Proposition 3.1), and (ii) all polynomials satisfying this condition belong to $\Lambda$ (Proposition 3.4). The former of these results makes use of the notion of a VWDWO sequence introduced in [3], while the latter is a linear-algebra calculation using the basis for $\Lambda_{(p)}$ constructed in [2]. In Section 4 we discuss the localizations of $\Lambda$ considered in [2] and show that as graded rings each is isomorphic to a graded version of a certain ring of integer-valued polynomials. Finally in Section 5 we show that the Abel formal group law over the ring $(\Lambda \otimes \mathbb{Z}_{(2)})[(a+b)^{-1}]$ is multiplicative.

[*] Corresponding author.
*E-mail addresses:* F.Clarke@Swansea.ac.uk (F. Clarke), johnson@mathstat.dal.ca (K. Johnson).

0022-4049/$ – see front matter © 2008 Elsevier B.V. All rights reserved.
doi:10.1016/j.jpaa.2008.11.031

## 2. A characterization of the ring $\Lambda$

Recall from [2] that the Abel formal group law $F_{\mathrm{Ab}}(u, v)$ of (1.1) has exponential series

$$\exp_{\mathrm{Ab}}(u) = \frac{\mathrm{e}^{au} - \mathrm{e}^{bu}}{a - b} = \frac{\mathrm{e}^{\alpha u}}{\sqrt{\beta}} \sinh\left(\sqrt{\beta} u\right),$$

where

$$\begin{aligned} a &= \alpha + \sqrt{\beta}, \\ b &= \alpha - \sqrt{\beta}, \end{aligned} \qquad \text{and} \qquad \begin{aligned} \alpha &= (a+b)/2, \\ \beta &= (a-b)^2/4. \end{aligned}$$

Abel's name is associated to this formal group law because of his study [4] of the functional equation that this exponential satisfies. This was his first research paper, published in 1823.

The coefficients $\alpha_n$ of $F_{\mathrm{Ab}}(u, v)$ can be expressed as polynomials either in $\alpha$ and $\beta$ or in $a$ and $b$.

**Proposition 2.1** (*Proposition 3.1 of [2]*). *$\alpha_1 = 2\alpha$, and if $n > 1$,*

$$\alpha_n = \begin{cases} \dfrac{-1}{(2\ell)!(2\ell-1)} \displaystyle\prod_{k=1}^{\ell} \left((2\ell-1)^2\alpha^2 - (2k-1)^2\beta\right), & \text{if } n = 2\ell, \\ \dfrac{\alpha}{(2\ell+1)!} \displaystyle\prod_{k=1}^{\ell} \left((2\ell)^2\alpha^2 - (2k)^2\beta\right), & \text{if } n = 2\ell+1. \quad \square \end{cases}$$

**Corollary 2.2.** *$\alpha_1 = a + b$, and if $n > 1$,*

$$\alpha_n = \frac{(-1)^{n-1}}{n!(n-1)} \prod_{\substack{i+j=n-1 \\ i,j \geq 0}} (ia + jb). \quad \square$$

Thus $\Lambda$ is the subring of $\mathbb{Q}[a, b]$ generated by the $\alpha_n$. They satisfy the following set of relations:

**Proposition 2.3** (*Lemma 3.3 of [2]*).

(i) *For $n \geq 3$,*

$$n\alpha_n + \sum_{k=2}^{n-1} k\alpha_k\alpha_{n-k} = 0.$$

(ii) *For $m, n \geq 2$,*

$$\alpha_m\alpha_n = \binom{m+n}{n}\alpha_{m+n} + \sum_{k=2}^{m+n-1} \left[F_{\mathrm{Ab}}(u, v)^k\right]_{m,n} \alpha_k,$$

*where $\left[F_{\mathrm{Ab}}(u, v)^k\right]_{m,n}$ denotes the coefficient in $F_{\mathrm{Ab}}(u, v)^k$ of $u^m v^n$.*

The main result of this paper is the following "numerical" characterization of $\Lambda$.

**Theorem 2.4.** *The ring $\Lambda$ consists of those symmetric polynomials in $\mathbb{Q}[a, b]$ such that $f(kt, \ell t) \in \mathbb{Z}[t, (k-\ell)^{-1}]$ for any integers $k, \ell$ such that $k \neq \ell$.*

## 3. The proof of Theorem 2.4

We show first that the integrality condition is satisfied by all polynomials in $\Lambda$.

**Proposition 3.1.** *If $f(a, b) \in \Lambda \subseteq \mathbb{Q}[a, b]$, then, for any $k \neq \ell \in \mathbb{Z}$,*

$$f(kt, \ell t) \in \mathbb{Z}[t, (k-\ell)^{-1}].$$

**Proof.** First note that it suffices to verify the assertion for homogeneous polynomials $f \in \Lambda$, for which the condition is equivalent to showing that $f(k, \ell) \in \mathbb{Z}_{(p)}$ for each prime $p$ and each $k, \ell \in \mathbb{Z}$ with $p \nmid (k - \ell)$.

Moreover, since the generators $\alpha_n$ are all homogeneous, it suffices to show that they satisfy this condition. Recall, from [3], that a sequence of integers $\{a_i\}$ is called a VWDWO (very well distributed and well ordered) sequence for a prime $p$ if $\nu_p(a_i - a_j) = \nu_p(i - j)$ for all $i, j$, where $\nu_p(x)$ denotes the $p$-adic valuation of $x$.

For such a sequence

$$\nu_p\left(\prod_{i=k}^{n+k-1} a_i\right) \geq \sum_{i\geq 0} \lfloor n/p^i \rfloor = \nu_p(n!), \tag{3.2}$$

for any $n$ and $k$. Also, if $\{a_i\}$ is a sequence such that for any $k$ and $\ell$ the set $\left\{a_{i+k} : i = 0, 1, \ldots, p^\ell - 1\right\}$ is a complete set of residue classes modulo $p^\ell$, then it is a VWDWO sequence for $p$. If $r$ and $s$ are such that $p \nmid r$, then the sequence $\{s + rj : j \geq 0\}$ has this property. Therefore, given $n$, $k$ and $\ell$ with $p \nmid (k - \ell)$, the sequence $\{(n-1)\ell + j(k-\ell) : j \geq 0\}$ is VWDWO, so that

$$\nu_p\left(\prod_{j=0}^{n-1}(n-1)\ell + j(k-\ell)\right) = \nu_p\left(\prod_{\substack{i+j=n-1\\ i,j\geq 0}} i\ell + jk\right) \geq \nu_p(n!).$$

If $p \nmid (n-1)$, Corollary 2.2 now shows that $\alpha_n(k, \ell) \in \mathbb{Z}_{(p)}$. If $p \mid (n-1)$, then we write

$$\prod_{j=0}^{n-1}((n-1)\ell + j(k-\ell)) = \frac{(n-1)\ell}{(n-1)\ell + n(k-\ell)} \prod_{j=1}^{n}((n-1)\ell + j(k-\ell)),$$

so that, using (3.2) again,

$$\nu_p\left(\prod_{i+j=n-1} i\ell + jk\right) \geq \nu_p(n-1) + \nu_p(n!).$$

Hence $\alpha_n(k, \ell) \in \mathbb{Z}_{(p)}$ in this case also. □

To complete the proof of Theorem 2.4 we shall need the following description of the localization $\Lambda_{(p)} = \Lambda \otimes \mathbb{Z}_{(p)}$ of $\Lambda$ at a rational prime $p$. This result is also due to Bukhshtaber and Kholodov.

**Proposition 3.3** (*Theorem 3.3 and 3.2 of [2]*).

(i) *$\Lambda_{(2)}$ has a $\mathbb{Z}_{(2)}$-basis consisting of the monomials*

$$\alpha_1^n \alpha_2^{j_1} \alpha_4^{j_2} \cdots \alpha_{2^k}^{j_k}, \quad \text{for } 0 \leq n, 0 \leq j_i < 2.$$

(ii) *If $p$ is an odd prime, $\Lambda_{(p)}$ has a $\mathbb{Z}_{(p)}$-basis consisting of the monomials*

$$\alpha_1^n \alpha_2^m \alpha_p^{j_1} \alpha_{p^2}^{j_2} \cdots \alpha_{p^k}^{j_k}, \quad \text{for } 0 < n, 0 \leq m \leq \frac{p-3}{2}, 0 \leq j_i < p,$$

$$\alpha_2^m \alpha_p^{j_1} \alpha_{p^2}^{j_2} \cdots \alpha_{p^k}^{j_k}, \quad \text{for } 0 \leq m, 0 \leq j_i < p. \quad \square$$

Thus Theorem 2.4 will be proved if we can show

**Proposition 3.4.** *Let $p$ be a prime and $f(a, b) \in \mathbb{Q}[a, b]$ a symmetric, homogeneous polynomial such that*

$$f(k, \ell) \in \mathbb{Z}_{(p)}$$

*for all $k, \ell \in \mathbb{Z}$ with $p \nmid k - \ell$. Then $f$ is a $\mathbb{Z}_{(p)}$-linear combination of the monomials in Proposition 3.3.*

The proof of this proposition will occupy the rest of this section. We will evaluate $f$ and the basis monomials of Proposition 3.3 at a suitably chosen set of values, form the resulting system of linear equations to express $f$ in terms of the monomials, and show that this system is solvable over $\mathbb{Z}_{(p)}$ by showing that the coefficient matrix is invertible over $\mathbb{Z}_{(p)}$. The proof of this last assertion is separated into the case $p = 2$, which is fairly straightforward, and the case $p$ odd, which is not. Our plan requires some information about the values of the basis monomials.

**Proposition 3.5.** *If $\ell \equiv k + 1 \bmod p^{n+1}$ with $n > 0$, then*

$$\alpha_{p^n}(k, \ell) \equiv \lfloor k/p^n \rfloor - k \bmod p.$$

To prove this proposition we need the following lemma on binomial coefficients.

**Lemma 3.6.** *If $k \geq p^n$ and $\tilde{k} \equiv k \bmod p^n$ with $0 \leq \tilde{k} < p^n$, then*

$$\binom{k}{p^n} \frac{p^n}{k - \tilde{k}} \in 1 + p\mathbb{Z}_{(p)}.$$

*In particular,*

$$\binom{k}{p^n} \equiv \left\lfloor \frac{k}{p^n} \right\rfloor \bmod p.$$

**Proof.** We can write $\binom{k}{p^n}\frac{p^n}{k-\tilde{k}}$ as the product of

$$\prod_{i=1}^{\tilde{k}} \frac{k-\tilde{k}+i}{i} \quad \text{and} \quad \prod_{i=\tilde{k}+1}^{p^n-1} \frac{k-\tilde{k}-p^n+i}{i},$$

within which each factor belongs to $1+p\mathbb{Z}_{(p)}$. For the last part, note that $\left\lfloor \frac{k}{p^n} \right\rfloor = \frac{k-\tilde{k}}{p^n}$. □

**Proof of Proposition 3.5.** Write $\ell = k - p^{n+1}N + 1$, and let $\tilde{k}$ be such that $0 \le \tilde{k} < p^n$ and $\tilde{k} \equiv k \bmod p^n$. Then

$$\begin{aligned}
\alpha_{p^n}(k,\ell) &= \frac{(-1)^{p^n-1}}{p^n!(p^n-1)} \prod_{j=0}^{p^n-1} \big((p^n-1-j)k + j(k-p^{n+1}N+1)\big) \\
&= \frac{(-1)^{p^n-1}}{p^n!(p^n-1)} \prod_{j=0}^{p^n-1} \big((p^n-1)(k-j) - jp^n(pN-1)\big) \\
&\equiv \frac{(-1)^{p^n-1}}{p^n!(p^n-1)} \left( \prod_{j=0}^{p^n-1} (p^n-1)(k-j) - \tilde{k}p^n(pN-1) \prod_{\substack{j=0 \\ j\neq\tilde{k}}}^{p^n-1} (p^n-1)(k-j) \right) \bmod p,
\end{aligned}$$

since $\nu_p(k-j) < n$ unless $j = \tilde{k}$.

The result now follows from Lemma 3.6, for we may write the last expression as

$$(1-p^n)^{p^n-1}\binom{k}{p^n}\left(1 + \frac{\tilde{k}p^n(pN-1)}{(1-p^n)(k-\tilde{k})}\right) \equiv \left\lfloor \frac{k}{p^n} \right\rfloor - k \bmod p. \quad \square$$

With this result about certain values of the $\alpha_{p^n}$ in hand, we may prove Proposition 3.4, considering first the case $p = 2$, for which Proposition 3.5 specializes to

**Corollary 3.7.** *If $L > n$, then*

$$\alpha_{2^n}(2k, 2k-2^L+1) \equiv \left\lfloor k/2^{n-1} \right\rfloor \bmod 2. \quad \square$$

It follows that

**Corollary 3.8.** *If $0 < i_1 < i_2 < \cdots < i_\ell < L$ and $i = \sum_{j=1}^{\ell} 2^{i_j-1}$, then*

$$\alpha_{2^{i_1}}\alpha_{2^{i_2}}\cdots\alpha_{2^{i_\ell}}(2k, 2k-2^L+1) \equiv \begin{cases} 0 \bmod 2, & \text{if } 0 \le k < i, \\ 1 \bmod 2, & \text{if } k = i. \end{cases}$$

**Proof.** If $k < i$, there is at least one $j$ such that the coefficient of $2^{i_j}$ in the base 2 expansion of $2k$ is zero, in which case $\alpha_{2^{i_j}}(2k, 2k-2^L+1) \equiv \left\lfloor k/2^{i_j-1} \right\rfloor \equiv 0 \bmod 2$.

On the other hand, $\alpha_{2^{i_j}}(2i, 2i-2^L+1) \equiv \left\lfloor i/2^{i_j-1} \right\rfloor \equiv 1 \bmod 2$, for each $1 \le j \le \ell$. □

Now fix $N$, choose $L$ such that $2^L > N$, and let $M_2$ denote the $(\lfloor N/2 \rfloor + 1) \times (\lfloor N/2 \rfloor + 1)$ matrix with $(i,k)$-entry

$$\alpha_1^{N-2i}\alpha_{2^{i_1}}\alpha_{2^{i_2}}\cdots\alpha_{2^{i_\ell}}(2k, 2k-2^L+1),$$

where $2i = \sum_{j=1}^{\ell} 2^{i_j}$.

**Lemma 3.9.** *The matrix $M_2$ is upper triangular modulo 2 , with diagonal elements all congruent to 1 modulo 2 .*

**Proof.** This follows from Corollary 3.8, together with the fact that $\alpha_1(2k, 2k-2^L+1) = 4k-2^L+1$ is odd. □

Now suppose $f(a,b)$ satisfies the hypotheses of Proposition 3.4 with $p = 2$, and let $N$ be its degree. Since $\Lambda \otimes \mathbb{Q} = \mathbb{Q}[a,b]^{S_2}$, the basis elements of Proposition 3.3(i) of degree $N$ provide a $\mathbb{Q}$-basis for the vector space of homogeneous symmetric polynomials of degree $N$. Thus we may write $f(a,b)$ as $\sum_{i=0}^{\lfloor N/2 \rfloor} c_i\,\alpha_1^{N-2i}\alpha_{2^{i_1}}\alpha_{2^{i_2}}\cdots\alpha_{2^{i_\ell}}$, where $2i = \sum_{j=1}^{\ell} 2^{i_j}$ and $c_i \in \mathbb{Q}$. Evaluating at $\left\{(2k, 2k-2^L+1) : 0 \le k \le \lfloor N/2 \rfloor\right\}$ gives a linear system of equations for the $c_i$ whose coefficient matrix is $M_2$, which is invertible over $\mathbb{Z}_{(2)}$, by Lemma 3.9. Thus, since the values of $f(a,b)$ belong to $\mathbb{Z}_{(2)}$, so do the $c_i$.

This completes the proof of Proposition 3.4 for the case $p = 2$. □

The case $p > 2$, to which we now turn, is complicated by the fact that the analogous matrix $M_p$ is not upper triangular modulo $p$. We will show, however, that it is still invertible, which suffices for our purposes.

For a given $N > 0$, we divide the basis elements in Proposition 3.3(ii) into subsets as follows: For each $m = 0, 1, \dots, (p-3)/2$, let

$$\mathscr{P}_m = \left\{ \alpha_1^n \alpha_2^m \alpha_p^{j_1} \dots \alpha_{p^\ell}^{j_\ell} : 0 < n, 0 \le j_i < p, n + 2m + \sum j_i p^i = N \right\},$$

and let

$$\mathscr{Q} = \left\{ \alpha_2^m \alpha_p^{j_1} \dots \alpha_{p^\ell}^{j_\ell} : 0 \le m, 0 \le j_i < p, 2m + \sum j_i p^i = N \right\}.$$

Note that these subsets are disjoint and together include all of the basis elements of degree $N$ listed in Proposition 3.3(ii), of which there are $\lfloor N/2 \rfloor + 1$.

We consider first the special case $N = p^\ell - 1$, for which $|\mathscr{P}_m| = p^{\ell-1}$ for all $m$, and $|\mathscr{Q}| = (p^{\ell-1} - 1)/2$. Choose $L > \ell$, and define sets $P_m, Q \subset \mathbb{Z}^2$ as follows:

For each $m = 0, 1, \dots, (p-3)/2$, let

$$P_m = \left\{ (kp + m, kp + m - p^L + 1) : 0 \le k \le p^{\ell-1} - 1 \right\},$$

and let

$$Q = \left\{ \left( kp + \frac{p-1}{2}, kp + \frac{p-1}{2} - p^L + 1 \right) : 0 \le k \le (p^{\ell-1} - 1)/2 \right\}.$$

Let $M_p$ be the matrix obtained by evaluating the basis elements in $\bigcup_m \mathscr{P}_m \cup \mathscr{Q}$ at the values $\bigcup_m P_m \cup Q$. We order the columns of $M_p$, corresponding to the elements of $\bigcup_m P_m \cup Q$ by arranging the $P_m$ in blocks by increasing $m$, followed by $Q$, and within each of these blocks ordering by increasing $k$. We order the rows of $M_p$ corresponding to the elements of $\bigcup_m \mathscr{P}_m \cup \mathscr{Q}$ by arranging the $\mathscr{P}_m$'s in blocks by increasing $m$, followed by $\mathscr{Q}$, and within each block ordering by increasing value of $\sum j_i p^i$. The result of this is a matrix $M_p$ made up of the following blocks: the $p^{\ell-1} \times p^{\ell-1}$ submatrices $\mathscr{P}_m(P_{m'})$ for $0 \le m, m' \le (p-3)/2$, which form a submatrix which we denote $\mathscr{P}(P)$, the $(p^{\ell-1}+1)/2 \times (p^{\ell-1}+1)/2$ submatrix $\mathscr{Q}(Q)$, and the non-square blocks $\mathscr{P}_m(Q)$ and $\mathscr{Q}(P_{m'})$. Thus

$$M_p = \begin{pmatrix} \mathscr{P}_1(P_1) & \cdots & \mathscr{P}_1(P_{(p-3)/2}) & \mathscr{P}_1(Q) \\ \vdots & \ddots & \vdots & \vdots \\ \mathscr{P}_{(p-3)/2}(P_1) & \cdots & \mathscr{P}_{(p-3)/2}(P_{(p-3)/2}) & \mathscr{P}_{(p-3)/2}(Q) \\ \mathscr{Q}(P_1) & \cdots & \mathscr{Q}(P_{(p-3)/2}) & \mathscr{Q}(Q) \end{pmatrix}.$$

A useful preliminary observation is

**Lemma 3.10.**

$$\alpha_1(kp + m, kp + m - p^L + 1) \equiv 2m + 1 \bmod p,$$
$$\alpha_2(kp + m, kp + m - p^L + 1) \equiv -\tfrac{m(m+1)}{2} \bmod p. \quad \square$$

**Corollary 3.11.** $\mathscr{P}_m(Q) = 0$ *for* $0 \le m \le (p-3)/2$.

**Proof.** Each element of $\mathscr{P}_m$ contains $\alpha_1$ as a factor, and $\alpha_1(Q) = 0$ by the lemma. □

Thus the problem of showing that $M_p$ is invertible modulo $p$ decomposes into that of studying $\mathscr{P}(P)$ and $\mathscr{Q}(Q)$ separately. We begin with $\mathscr{P}(P)$.

**Lemma 3.12.** *If* $k = \sum_{i=0}^{\ell-1} k_i p^i$, *the entries of the submatrix* $\mathscr{P}_m(P_{m'})$ *are, modulo p,*

$$\begin{aligned} \alpha_1^n \alpha_2^m \alpha_p^{j_1} \dots \alpha_{p^\ell}^{j_\ell}(kp + m', kp + m' - p^L + 1) &\equiv (2m'+1)^n (-m'(m'+1)/2)^m \prod_{i=1}^{\ell} (k_{i-1} - m')^{j_i} \\ &\equiv \left( \frac{-m'(m'+1)}{2(2m'+1)^2} \right)^m \prod_{i=1}^{\ell} \left( \frac{k_{i-1} - m'}{2m'+1} \right)^{j_i}. \end{aligned}$$

**Proof.** The first congruence follows directly from Proposition 3.5 and Lemma 3.10, while the second follows from noting that $(2m'+1)^n \equiv (2m'+1)^{-2m}(2m'+1)^{\sum j_i} \bmod p$ since $n = (p^\ell - 1) - 2m - \sum j_i p^i$. □

**Corollary 3.13.**

$$\mathscr{P}_m(P_{m'}) = \left( \frac{-m'(m'+1)}{2(2m'+1)^2} \right)^m \mathscr{P}_0(P_{m'}). \quad \square$$

We consider next how $\mathcal{P}_0(P_{m'})$ depends on $m'$. Given $0 \leq m' \leq (p-3)/2$, define a permutation $\varphi$ of $\{0, 1, \ldots, p^\ell - 1\}$ by $\varphi(k) \equiv (k - m')/(2m'+1) \bmod p$ if $k < p$, and by $\varphi(\sum k_i p^i) = \sum \varphi(k_i) p^i$ if $0 \leq k_i < p$. It follows that

**Lemma 3.14.** *The matrix $\mathcal{P}_0(P_{m'})$ is equal to the matrix $\mathcal{P}_0(P_0)$ with its columns permuted by $\varphi$.* □

Combining Lemmas 3.12 and 3.14, we have

**Proposition 3.15.** *The permutation of the columns of the matrix $\mathcal{P}(P)$, given by the function $\varphi$ above, yields a matrix congruent modulo $p$ to the tensor product of the matrices*

$$\left(\left(\frac{-m'(m'+1)}{2(2m'+1)^2}\right)^m\right)_{0 \leq m, m' \leq (p-3)/2}$$

*and*

$$\mathcal{P}_0(P_0) = \left(\prod_{i=1}^{\ell-1} k_{i-1}^{j_i}\right)_{0 \leq k_{i-1}, j_i < p}.$$

*The latter matrix is itself equal to the $(\ell-1)$-fold tensor power of*

$$\left(k^j\right)_{0 \leq k, j < p}. \quad \square$$

**Corollary 3.16.** *$\mathcal{P}(P)$ is invertible modulo $p$.*

**Proof.** The matrices in the proposition are Vandermonde matrices with non-zero determinant modulo $p$. Hence the tensor product is invertible modulo $p$. □

We turn now to $\mathcal{Q}(Q)$.

**Lemma 3.17.** *If $k = \sum_{i=0}^{\ell-1} k_i p^i$, then the entries in the submatrix $\mathcal{Q}(Q)$ are, modulo $p$,*

$$\begin{aligned}\alpha_2^m \alpha_p^{j_i} \cdots \alpha_{p^\ell}^{j_\ell}\left(kp + \frac{p-1}{2}, kp + \frac{p-1}{2} - p^L + 1\right) &\equiv 2^{-3m} \prod_{i=1}^{\ell}\left(k_{i-1} + \frac{1}{2}\right)^{j_i} \\ &\equiv \varepsilon^\ell \prod_{i=1}^{\ell}\left(\varepsilon^{i-1}(2k_{i-1}+1)z\right)^{j_i},\end{aligned}$$

*where $z \in \mathbb{F}_{p^2}$ is such that $z^2 = 2$ and $\varepsilon$ is the Legendre symbol $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$.*

**Proof.** The first formula follows as for Lemma 3.12 once we note that

$$\alpha_2\left(kp + \frac{p-1}{2}, kp + \frac{p-1}{2} - p^L + 1\right) \equiv 1/8 \bmod p.$$

Now $z^p = \varepsilon z$ and $z^3 = 2z$. As $2m = p^\ell - 1 - pj$, where $j = \sum j_i p^{i-1}$ and $j$ is even, we have $2^{-3m} = z^{-6m} = \varepsilon^\ell 2^j z^j$ in $\mathbb{F}_{p^2}$. Since $2^{p^{i-1}} = 2$ and $z^{p^{i-1}} = \varepsilon^{i-1} z$, the second formula follows. □

The $(p^{\ell-1}+1)/2 \times (p^{\ell-1}+1)/2$ matrix $\mathcal{Q}(Q)$ consists (modulo $p$) of those entries in Lemma 3.17 for which $0 \leq k \leq (p^{\ell-1}-1)/2$ and $0 \leq \sum j_i p^i < p^{\ell-1}$ with $\sum j_i$ is even. Note that the latter condition ensures that in all cases the final expression in the lemma does indeed belong to $\mathbb{F}_p$.

In order to show that $\mathcal{Q}(Q)$ is invertible, we embed its mod $p$ reduction in the $p^{\ell-1} \times p^{\ell-1}$ matrix $\overline{\mathcal{Q}(Q)}$ (defined over $\mathbb{F}_p$ or $\mathbb{F}_{p^2}$ as appropriate) having entries $\varepsilon^r \prod_{i=1}^{\ell}\left(\varepsilon^{i-1}(2k_{i-1}+1)z\right)^{j_i}$, where now $0 \leq k < p^{\ell-1}$ and $0 \leq \sum j_i p^i < p^{\ell-1}$ without requiring that $\sum j_i$ is even. Thus all values of $k_i, j_i$ satisfying $0 \leq j_i, k_i < p$ arise. Now $\overline{\mathcal{Q}(Q)}$ is invertible since it is a Vandermonde matrices with non-zero determinant.

It follows that the $((p^{\ell-1}+1)/2) \times p^{\ell-1}$ matrix $A$ consisting of those rows of $\overline{\mathcal{Q}(Q)}$ for which $\sum j_i$ is even has rank $(p^{\ell-1}+1)/2$. If $\overline{k} = p^{\ell-1} - k - 1$, then $2\overline{k}_i + 1 = -(2k_i+1)$ for all $i$ and the column of $A$ corresponding to $\overline{k}$ is equal to the column corresponding to $k$. But since $A$ must have $(p^{\ell-1}+1)/2$ linearly independent columns, the matrix consisting of those columns of $A$ for which $0 \leq k \leq (p^{\ell-1}-1)/2$, to which $\mathcal{Q}(Q)$ is congruent modulo $p$, is invertible.

Hence we have proved.

**Proposition 3.18.** *For $N = p^\ell - 1$ the matrix $M_p$ is invertible.* □

We now consider the basis elements in a degree $N < p^\ell - 1$. Letting $\mathcal{P}$ and $\mathcal{Q}$ continue to denote the above sets of basis elements in degree $p^\ell - 1$, let $\widetilde{\mathcal{P}}$ and $\widetilde{\mathcal{Q}}$ denote the corresponding sets of basis elements in degree $N$.

Multiplication by $\alpha_1^{p^\ell-N-1}$ provides an injective map from $\widetilde{\mathscr{P}}$ to $\mathscr{P}$. Thus the matrix $\widetilde{\mathscr{P}}(P)$ obtained by evaluating the elements of $\widetilde{\mathscr{P}}$ on the pairs in $P$ can be obtained, modulo $p$, by choosing the corresponding rows of $\mathscr{P}(P)$ and multiplying each column by a scalar which (by Lemma 3.10) is non-zero. Since, by Corollary 3.16, $\mathscr{P}(P)$ has maximum rank modulo $p$, so does $\widetilde{\mathscr{P}}(P)$, and it is possible to choose a subset $\widetilde{P} \subset P$ for which the matrix $\widetilde{\mathscr{P}}(\widetilde{P})$ is invertible.

If $N$ is even, multiplication by $\alpha_2^{(p^\ell-N-1)/2}$ is an injection $\widetilde{\mathscr{Q}} \to \mathscr{Q}$. If $N$ is odd, an injection $\widetilde{\mathscr{Q}} \to \mathscr{Q}$ is provided by sending $\alpha_2^{\widetilde{m}}\alpha_p^{\widetilde{j}_1}\alpha_{p^2}^{\widetilde{j}_2}\ldots\alpha_{p^{\ell-1}}^{\widetilde{j}_\ell}$ to $\alpha_2^{m}\alpha_p^{j_1}\alpha_{p^2}^{j_2}\ldots\alpha_{p^{\ell-1}}^{j_\ell}$, where $m = \widetilde{m} + (p^\ell - N - p - 1)/2$ and $\sum j_ip^i = 1 + \sum \widetilde{j}_ip^i$ with $0 \le \widetilde{j}_i, j_i < p$. In both cases the same argument as above shows that there is a subset $\widetilde{Q} \subset Q$ for which $\widetilde{\mathscr{Q}}(\widetilde{Q})$ is invertible.

With the sets $\widetilde{P}$, $\widetilde{Q}$ constructed in this way we may form the degree $N$ matrix

$$M_p = \begin{pmatrix} \widetilde{\mathscr{P}}(\widetilde{P}) & \widetilde{\mathscr{P}}(\widetilde{Q}) \\ \widetilde{\mathscr{Q}}(\widetilde{P}) & \widetilde{\mathscr{Q}}(\widetilde{Q}) \end{pmatrix}$$

and have

**Proposition 3.19.** *In all degrees the matrix $M_p$ is invertible.* □

The proof of Proposition 3.4 now follows for $p$ odd just as in the case $p = 2$. This completes the proof of Theorem 2.4. □

## 4. Localizations of $\Lambda$

In [2, Theorem 4.3] Bukhshtaber and Kholodov considered three extensions of the ring $\Lambda$, each obtained by inverting various elements. We denote these rings by $A = \Lambda_{(2)}[(a+b)^{-1}]$, $B = \Lambda[\frac{1}{2}][(a-b)^{-2}]$ and $C = \Lambda[(a^2-b^2)^{-2}]$. The description of $\Lambda$ in Theorem 2.4 yields the following characterizations in terms of integrality conditions.

**Proposition 4.1.**

(i) $A = \left\{f(a,b) \in \mathbb{Q}[a,b,(a+b)^{-1}] : f(a,b) = f(b,a), f(kt,\ell t) \in \mathbb{Z}_{(2)}[t,t^{-1}] \text{ if } k,\ell \in \mathbb{Z} \text{ and } k-\ell \text{ is odd}\right\}$;

(ii) $B = \left\{f(a,b) \in \mathbb{Q}\left[a,b,(a-b)^{-2}\right] : f(a,b) = f(b,a), f(kt,\ell t) \in \mathbb{Z}\left[\frac{1}{2},\frac{1}{k-\ell}\right][t,t^{-1}] \text{ if } k \ne \ell \in \mathbb{Z}\right\}$;

(iii) $C = \left\{f(a,b) \in \mathbb{Q}\left[a,b,(a^2-b^2)^{-2}\right] : f(a,b) = f(b,a), f(kt,\ell t) \in \mathbb{Z}\left[\frac{1}{k^2-\ell^2}\right][t,t^{-1}] \text{ if } k \ne \pm\ell \in \mathbb{Z}\right\}$. □

But we can describe these rings still more explicitly in terms of integer-valued polynomials. We consider $A$ and $C$ first, since the ring $B$ turns out to be rather more complicated.

Let $\mathrm{Int}(\mathbb{Z}_{(2)}) = \left\{f(x) \in \mathbb{Q}[x] : f(\mathbb{Z}_{(2)}) \subseteq \mathbb{Z}_{(2)}\right\}$ be the ring of 2-local integer-valued polynomials. Give $A$ the grading in which $|a| = |b| = 2$, and let $\mathrm{Int}(\mathbb{Z}_{(2)})[y,y^{-1}]$ have grading with $|x| = 0$ and $|y| = 2$.

**Proposition 4.2.** *$A = \Lambda_{(2)}[(a+b)^{-1}]$ and $\mathrm{Int}(\mathbb{Z}_{(2)})[y,y^{-1}]$ are isomorphic as graded rings.*

**Proof.** If $k,\ell \in \mathbb{Z}$ have different parity, then $\frac{k\ell}{2(k+\ell)^2} \in \mathbb{Z}_{(2)}$. Hence we may define a ring homomorphism $\mathrm{Int}(\mathbb{Z}_{(2)}) \to A$ by $f(x) \mapsto f\left(\frac{ab}{2(a+b)^2}\right)$.

It will be sufficient to show that $\mathrm{Int}(\mathbb{Z}_{(2)})$ maps isomorphically onto the component $A_0$ of degree zero. For then this isomorphism can be extended to $\mathrm{Int}(\mathbb{Z}_{(2)})[y,y^{-1}]$ by sending $y$ to $a+b$.

Since $\Lambda \otimes \mathbb{Q}$ is the symmetric algebra $\mathbb{Q}[a,b]^{S_2} = \mathbb{Q}[a+b,ab]$, the degree-zero component of $A \otimes \mathbb{Q}$ is the polynomial ring $\mathbb{Q}\left[\frac{ab}{(a+b)^2}\right]$. Thus every element of $A_0$ may be written (uniquely) in the form $f(\frac{ab}{2(a+b)^2})$ for some polynomial $f(x) \in \mathbb{Q}[x]$. We need to show that $f(x) \in \mathrm{Int}(\mathbb{Z}_{(2)})$. If $\ell = 1-k$, then $\frac{k\ell}{2(k+\ell)^2} = \frac{k(1-k)}{2} \in \mathbb{Z}$, so $f$ is certainly $\mathbb{Z}_{(2)}$-valued on the triangular numbers $\left\{\frac{k(1-k)}{2} : k \in \mathbb{Z}\right\}$.

However, the triangular numbers are 2-adically dense in $\mathbb{Z}_{(2)}$. For if $\frac{k(1-k)}{2} = r \in \mathbb{Z}_2$, then $k = \frac{1\pm\sqrt{1-8r}}{2}$ in $\mathbb{Q}_2$. But the two square roots of $1-8r$ belong to $1+2\mathbb{Z}_2$, so that the solutions for $k$ belong to $\mathbb{Z}_2$. It follows that $f$ is $\mathbb{Z}_{(2)}$-valued on the whole of $\mathbb{Z}_{(2)}$. □

Let $T = \mathrm{Int}(\mathbb{Z}^{(2)},\mathbb{Z})$ be the ring

$$\left\{f(x) \in \mathbb{Q}[x] : f(r^2) \in \mathbb{Z} \text{ for all } r \in \mathbb{Z}\right\}$$

of polynomials integer-valued on the set $\mathbb{Z}^{(2)}$ of squares of integers, and let

$$T[x^{-1}] = \left\{f(x) \in \mathbb{Q}\left[x,x^{-1}\right] : f(r^2) \in \mathbb{Z}\left[\frac{1}{r}\right] \text{ for all } r \in \mathbb{Z} \setminus \{0\}\right\}$$

be its localization away from $x$.

**Proposition 4.3.** *The graded ring $C$ is isomorphic to $T[x^{-1}][y,y^{-1}]$, where $|x| = 0$ and $|y| = 2$.*

**Proof.** Note that since $(a^2-b^2)^2 = (a+b)^2(a-b)^2$ is invertible in $C$, so are $a+b$ and $(a-b)^2$. Define a ring homomorphism $T[x^{-1}][y, y^{-1}] \to \mathbb{Q}[a, b, (a^2-b^2)^{-2}]$ by sending $x \mapsto \left(\frac{a+b}{a-b}\right)^2$ and $y \mapsto a+b$. It will be sufficient to show that this maps $T[x^{-1}]$ isomorphically onto the degree-zero component $C_0$.

If $h(x) \in T[x^{-1}]$, then there exists $n \geq 0$ such that $h(x) = x^n g(x)$ with $g(x) \in T = \mathrm{Int}(\mathbb{Z}^{(2)}, \mathbb{Z})$. By a $p$-adic density argument $g(x) \in \mathrm{Int}(\mathbb{Z}_{(p)}^{(2)}, \mathbb{Z}_{(p)})$ for all primes $p$. Thus if $k, \ell \in \mathbb{Z}$ and $p$ is a prime which does not divide $k^2-\ell^2$, we have $g\left(\left(\frac{k+\ell}{k-\ell}\right)^2\right) \in \mathbb{Z}_{(p)}$ since $p \nmid k-\ell$, and then $h\left(\left(\frac{k+\ell}{k-\ell}\right)^2\right) \in \mathbb{Z}_{(p)}$ since $p \nmid k+\ell$. Hence $h\left(\left(\frac{a+b}{a-b}\right)^2\right) \in C_0$.

Suppose now that $f\left(\left(\frac{a+b}{a-b}\right)^2\right) \in C_0$, so that $f\left(\left(\frac{k+\ell}{k-\ell}\right)^2\right) \in \mathbb{Z}[\frac{1}{k^2-l^2}]$ for all $k, \ell \in \mathbb{Z}$ such that $k \neq \pm\ell$. Given an even integer $r$, let $k = r+1$ and $\ell = r-1$, so that $\frac{k+\ell}{k-\ell} = r$, $k^2-\ell^2 = 2r$, and $h(r^2) \in \mathbb{Z}[\frac{1}{2r}] = \mathbb{Z}[\frac{1}{r}]$. While if $r$ is odd, letting $k = (r+1)/2$ and $\ell = (r-1)/2$ yields directly $h(r^2) \in \mathbb{Z}[\frac{1}{r}]$. Hence $h(x) \in T[x^{-1}]$. □

We grade the ring $B$ in the same way as $A$ and $C$, and let $R = \mathrm{Int}(\mathbb{Z}[\frac{1}{2}]^{(2)}, \mathbb{Z}[\frac{1}{2}])$ denote the ring

$$\left\{f(x) \in \mathbb{Q}[x] : f(r^2) \in \mathbb{Z}\left[\frac{1}{2}\right] \text{ for all } r \in \mathbb{Z}\left[\frac{1}{2}\right]\right\}$$

of polynomials which are $\mathbb{Z}[\frac{1}{2}]$-valued on squares in $\mathbb{Z}[\frac{1}{2}]$.

**Lemma 4.4.** *The degree-zero component $B_0$ of the ring $B$ is isomorphic to $R$.*

**Proof.** We have $B \otimes \mathbb{Q} = \mathbb{Q}[a+b, ab, (a-b)^{-2}]$, and $ab = \left((a+b)^2-(a-b)^2\right)/4$. Thus $B \otimes \mathbb{Q} = \mathbb{Q}[a+b, (a-b)^2, (a-b)^{-2}]$, and $B_0 \otimes \mathbb{Q} = \mathbb{Q}\left[\left(\frac{a+b}{a-b}\right)^2\right]$. Thus

$$B_0 = \left\{f\left(\left(\frac{a+b}{a-b}\right)^2\right) : f(x) \in \mathbb{Q}[x] \text{ with } f\left(\left(\frac{k+\ell}{k-\ell}\right)^2\right) \in \mathbb{Z}\left[\frac{1}{2(k-\ell)}\right] \text{ if } k \neq \ell \in \mathbb{Z}\right\}.$$

If $f(x) \in R$, then, by a density argument, $f(x) \in \mathrm{Int}(\mathbb{Z}_{(p)}^{(2)}, \mathbb{Z}_{(p)})$ for all odd primes. Thus if $p$ is an odd prime which does not divide $k-\ell$, then $f\left(\left(\frac{k+\ell}{k-\ell}\right)^2\right) \in \mathbb{Z}_{(p)}$. This shows that $f\left(\left(\frac{a+b}{a-b}\right)^2\right) \in B_0$.

Conversely, given $f\left(\left(\frac{a+b}{a-b}\right)^2\right) \in B_0$, setting $k = s+2^m$ and $\ell = s-2^m$, where $s \in \mathbb{Z}$, yields $\frac{k+\ell}{k-\ell} = \frac{s}{2^m}$, and hence $f\left(\left(\frac{s}{2^m}\right)^2\right) \in \mathbb{Z}[\frac{1}{2}]$, so that $f(x) \in R$. □

Now let

$$J = \left\{g(x) \in \mathbb{Q}[x] : rg(r^2) \in \mathbb{Z}\left[\frac{1}{2}\right] \text{ for all } r \in \mathbb{Z}\left[\frac{1}{2}\right]\right\}.$$

This is an $R$-module, and $xJ$ is an ideal of $R$.

**Proposition 4.5.** *The graded ring $B$ is isomorphic to the ring defined as $(R \oplus yJ)[z, z^{-1}]$ subject to the relation $y^2 = xz$, where $|y| = 2$ and $|z| = 4$.*

**Proof.** If $g(x) \in J$ and $k \neq \ell$, then $(k+\ell)g\left(\left(\frac{k+\ell}{k-\ell}\right)^2\right) \in \mathbb{Z}\left[\frac{1}{2(k-\ell)}\right]$, so that we may extend the isomorphism $R \to B_0$ of Lemma 4.4, which sends $x$ to $(a+b)^2/(a-b)^2$, by sending $y$ to $a+b$ and $z$ to $(a-b)^2$.

Since both rings are periodic, under multiplication by $z$ and $(a-b)^2$, respectively, it remains only to show that we have an isomorphism in degree 2. It is clear that

$$B_2 = \left\{(a+b)g\left(\left(\frac{a+b}{a-b}\right)^2\right) : g(x) \in \mathbb{Q}[x] \text{ with } (k+\ell)g\left(\left(\frac{k+\ell}{k-\ell}\right)^2\right) \in \mathbb{Z}\left[\frac{1}{2(k-\ell)}\right] \text{ if } k \neq \ell \in \mathbb{Z}\right\}.$$

Given $(a+b)g\left(\left(\frac{a+b}{a-b}\right)^2\right) \in B_2$, set $k = s+2^m$ and $\ell = s-2^m$, then we have $2sg\left(\left(\frac{s}{2^m}\right)^2\right) \in \mathbb{Z}[\frac{1}{2}]$, so that $g(x) \in J$, and $(a+b)g\left(\left(\frac{a+b}{a-b}\right)^2\right)$ is the image of $yg(x)$. □

## 5. The formal group law over the ring $A$

The ring $A$ is of particular interest because of its resemblance to the coefficient ring of complex $K$-theory, with $a+b$ playing the role of the Bott element. To make this precise we note that

**Proposition 5.1.** *Let $\psi : \mathbb{Z}[t^{\pm 1}] \to A = \Lambda_{(2)}[(a+b)^{-1}]$ be defined by $\psi(t) = a + b$, and let*

$$\exp_{\mathrm{Ab}}(u) = \frac{\mathrm{e}^{au} - \mathrm{e}^{bu}}{a-b} \quad \textit{and} \quad \log_{\psi_* K}(u) = \frac{\ln(1 + (a+b)u)}{a+b}$$

*denote the exponential of the Abel formal group law and the logarithm of the multiplicative formal group law over A, respectively. Then*

$$\exp_{\mathrm{Ab}} \circ \log_{\psi_* K}(u) \in A[[u]],$$

*i.e., over A the Abel formal group law is multiplicative.*

**Proof.** We have

$$\begin{aligned}\exp_{\mathrm{Ab}}(\log_{\psi_* K}(u)) &= \frac{\mathrm{e}^{a\log(1+(a+b)u)/(a+b)} - \mathrm{e}^{b\log(1+(a+b)u)/(a+b)}}{a-b} \\ &= \frac{(1+(a+b)u)^{a/(a+b)} - (1+(a+b)u)^{b/(a+b)}}{a-b} \\ &= \sum_{j\geq 0}\left(\binom{a/(a+b)}{j} - \binom{b/(a+b)}{j}\right)\frac{(a+b)^j}{a-b}u^j.\end{aligned}$$

The coefficients clearly lie in $\mathbb{Q}[a, b]^{S_2}$. Thus it suffices to verify that they satisfy the integrality condition in Proposition 4.1(i). Suppose $k, \ell \in \mathbb{Z}$ with $k \not\equiv \ell \bmod 2$. Then $k + \ell$ is odd, and so $\binom{k/(k+\ell)}{j}$ and $\binom{\ell/(k+\ell)}{j}$ belong to $\mathbb{Z}_{(2)}$. □

## References

[1] P. Busato, Realization of Abel's universal formal group law, Math. Z. 239 (2002) 527–561.

[2] V.M. Bukhshtaber, A.N. Kholodov, Formal groups, functional equations and generalized cohomology theories, Math. USSR Sbornik 181 (1990) 75–94. English transl., Math. S. B. 69 (1991) pp. 77–97.

[3] P.-J. Cahen, J.-L. Chabert, Integer-valued polynomials, in: Mathematical Surveys and Monographs, vol. 48, Amer. Math. Soc., Providence, RI, 1997.

[4] N.H. Abel, Méthode générale pour trouver des fonctions d'une seule quantité variable, lorsqu'une propriété de ces fonctions est exprimée par une équation entre deux variables, Magazin for Naturvidenskaberne 1 (1823) 216–229. reprinted in: L. Sylow, S. Lie (Eds.), Œuvres Complètes, vol. 1, Christiania, 1881.