STEENROD AND ADAMS OPERATIONS FROM EASY ALGEBRA

JIAHAO HU

Abstract. In this note, we calculate in details the automorphism group of the additive (resp. multiplicative) formal group law over $\mathbb{F}_p$ and relate it to Steenrod operations (resp. Adams operations) in topology. I do not claim originality of these results except perhaps for formulating the statement of Theorem 4.2.

1. Introduction

A (one-dimensional commutative) formal group law over a commutative ring R is a formal power series in two variables $F(x,y) \in R[[x,y]]$ that behaves like a (commutative) group multiplication. More precisely, F must satisfy

- $F(x,0) = x$ and $F(0,y) = y$
- $F(x,F(y,z)) = F(F(x,y),z)$
- $F(x,y) = F(y,x)$
- there exists $\mathrm{inv}(x) \in R[[x]]$ so that $F(x,\mathrm{inv}(x)) = F(\mathrm{inv}(x),x) = 0$

For example, $\mathbb{G}_a(x,y) = x+y$ and $\mathbb{G}_m(x,y) = x+y+xy$ are formal group laws over $\mathbb{Z}$ (and hence over any commutative ring with unit). $\mathbb{G}_a$ is called the additive formal group law, $\mathbb{G}_m$ is called the multiplicative formal group for $1+\mathbb{G}_m(x,y) = (1+x)(1+y)$.

For a more advanced example, let (E,O) be a smooth elliptic curve over R and let x be a local parameter near O, then the abelian group structure on E induces a formal group law over R. If one allows singularity, then if O is a nodal (resp. cusp) point, then the formal group law produced from E at O is isomorphic to $\mathbb{G}_m$ (resp. $\mathbb{G}_a$). In general, the formal group laws arising from elliptic curves are much more complicated.

Given a formal group law F over R, an endomorphism of F is a change of variable that preserves F. More precisely, an endomorphism is a power series $h \in R[[x]]$ such that $F(h(x),h(y)) = h(F(x,y))$. It is easy to see that h cannot have nonzero constant term, for $2c = c$ implies $c = 0$ in any ring (even in $\mathbb{F}_2$!).

We say an endomorphism is an automorphism if it is invertible as power series, or equivalently its coefficient of linear term is invertible in R. Denote the set of endomorphisms (resp. automorphisms) of F by $\mathrm{End}_R(F)$ (resp. $\mathrm{Aut}_R(F)$).

Our goal of this note is to determine $\mathrm{Aut}_R(\mathbb{G}_a)$ and $\mathrm{Aut}_R(\mathbb{G}_m)$ over the ring $R = \mathbb{F}_p$ where p is a prime, and relate them to Steenrod operations and Adams operations, both of which arise as cohomology operations, Steenrod for singular cohomology with $\mathbb{F}_p$-coefficients and Adams for complex K-theory.

2. Automorphism of additive group $\mathbb{G}_a$

We must solve the equation

$$f(x+y) = f(x) + f(y)$$

for power series $f(x) = a_0 x + a_1 x^2 + a_3 x^3 + \ldots$. This is equivalent to finding $a_0, a_1, a_2, \ldots$ so that

$$a_n \binom{n+1}{k} = 0$$

for all $n \geq 0$ and all $1 \leq k \leq n$.

By Bezout's theorem, for each n, the above is equivalent to

$$a_n \cdot \mathrm{gcd}_{1\leq k\leq n} \binom{n+1}{k} = 0$$

where $\mathrm{gcd}_{1\leq k\leq n}\binom{n+1}{k}$ is the greatest common divisor of $\binom{n+1}{1}, \binom{n+1}{2}, \ldots, \binom{n+1}{n}$.

It is an elementary (but quite non-trivial to me) fact that

$$\mathrm{gcd}_{1\leq k\leq n} \binom{n+1}{k} = \begin{cases} q, & \text{if } n+1 = q^s \text{ for some prime } q; \\ 1, & \text{otherwise.} \end{cases}$$

Now that we are working over $\mathbb{F}_p$, $\mathrm{gcd}_{1\leq k\leq n}\binom{n+1}{k}$ is invertible unless $n+1$ is a power of p. So f must have the form

$$f(x) = a_0 x + a_{p-1} x^p + a_{p^2-1} x^{p^2} + a_{p^3-1} x^{p^3} + \cdots$$

Rewrite $a_{p^k-1} =: \xi_k$, $k = 0, 1, 2, \ldots$, then we have

$$f(x) = \xi_0 x + \xi_1 x^p + \xi_2 x^{p^2} + \cdots + \xi_k x^{p^k} + \cdots$$

is a (infinite) linear combination of powers of the Frobenius map $x \mapsto x^p$. Since the Frobenius map preserves $\mathbb{G}_a$, the coefficients ξ_k can be arbitrarily chosen. Therefore, we have proven:

Proposition 2.1.

$$\mathrm{End}_{\mathbb{F}_p}(\mathbb{G}_a) \simeq \mathrm{Spec}\mathbb{F}_p[\xi_0, \xi_1, \xi_2, \ldots]$$

and

$$\mathrm{Aut}_{\mathbb{F}_p}(\mathbb{G}_a) \simeq \mathrm{Spec}\mathbb{F}_p[\xi_0, \xi_0^{-1}, \xi_1, \xi_2, \ldots].$$

Since $\mathrm{Aut}_{\mathbb{F}_p}(\mathbb{G}_a)$ is a group (under composition of power series), its group multiplication corresponds to a diagonal homomorphism

$$\mathbb{F}_p[\xi_0, \xi_0^{-1}, \xi_1, \xi_2, \ldots] \to \mathbb{F}_p[\xi_0, \xi_0^{-1}, \xi_1, \xi_2, \ldots] \otimes \mathbb{F}_p[\xi_0, \xi_0^{-1}, \xi_1, \xi_2, \ldots]$$

We shall describe the group structure on the subgroup $S\mathrm{Aut}_{\mathbb{F}_p}(\mathbb{G}_a)$ that consists of all automorphism of $\mathbb{G}_a$ whose linear term is x, i.e. $\xi_0 = 1$. Then it is clear $S\mathrm{Aut}(\mathbb{G}_a)_{\mathbb{F}_p} \simeq \mathrm{Spec}\mathbb{F}_p[\xi_1, \xi_2, \xi_3, \ldots]$ and we have a natural (split) exact sequence

$$1 \to S\mathrm{Aut}_{\mathbb{F}_p}(\mathbb{G}_a) \to \mathrm{Aut}_{\mathbb{F}_p}(\mathbb{G}_a) \xrightarrow{\xi_0} \mathbb{F}_p^* \to 1.$$

As before, the group multiplication on $S\mathrm{Aut}_{\mathbb{F}_p}(\mathbb{G}_a)$ corresponds to a diagonal morphism

$$\Delta : \mathbb{F}_p[\xi_1, \xi_2, \ldots] \to \mathbb{F}_p[\xi_1, \xi_2, \ldots] \otimes \mathbb{F}_p[\xi_1, \xi_2, \ldots].$$

To determine Δ, we must calculate the composition of two automorphisms of $\mathbb{G}_a$. Let $f(x) = \xi_0 x + \xi_1 x^p + \xi_2 x^{p^2} + \cdots$ and $g(x) = \xi_0' x + \xi_1' x^p + \xi_2' x^{p^2} + \cdots$ be two automorphism of $\mathbb{G}_a$, then

$$\begin{aligned} g \circ f(x) &= f(x) + \xi_1' f(x)^p + \xi_2' f(x)^{p^2} + \cdots \\ &= x + (\xi_1' + \xi_1)x^p + (\xi_2' + \xi_1^p \xi_1 + \xi_2)x^{p^2} + (\xi_3' + \xi_1^{p^2} \xi_2' + \xi_2^p \xi_1' + \xi_3)x^{p^3} + \cdots \\ &= \sum_{k=0}^{\infty} (\sum_{i=0}^{k} \xi_{k-i}^{p^i} \xi_i') x^k \quad (\text{recall } \xi_0 = 1) \end{aligned}$$

Therefore, we have

$$\Delta \xi_k = \sum_{i=0}^{k} \xi_{k-i}^{p^i} \otimes \xi_i. \tag{1}$$

The group inversion on $S\mathrm{Aut}_{\mathbb{F}_p}(\mathbb{G}_a)$ corresponds to a morphism

$$c : \mathbb{F}_p[\xi_1, \xi_2, \ldots] \to \mathbb{F}_p[\xi_1, \xi_2, \ldots].$$

To determine c, we assume g as above is the inverse of f, then we have

$$\sum_{i=0}^{k} \xi_{k-i}^{p^i} \xi_i' = 0 \quad \text{for } k \geq 1.$$

Therefore, c is inductively determined by the relations

$$\sum_{i=0}^{k} \xi_{k-i}^{p^i} \cdot c(\xi_i) = 0 \tag{2}$$

Proposition 2.2. *$\mathbb{F}_p[\xi_1, \xi_2, \xi_2 \ldots]$ is naturally a Hopf algebra whose co-multiplication is given by Δ and anti-automorphism is given by c. Moreover, it is commutative, co-associative but not co-commutative (as $S\mathrm{Aut}_{\mathbb{F}_p}(\mathbb{G}_a)$ is not commutative).*

I shall leave the calculation for $\mathrm{Aut}_{\mathbb{F}_p}(\mathbb{G}_a)$ to the interested reader (since I am lazy, sorry, but you know what to do).

3. Automorphism of multiplicative group $\mathbb{G}_m$

Similarly, we must solve the equation

$$f(x + y + xy) = f(x) + f(y) + f(x)f(y)$$

for power series $f(x) = a_1 x + a_2 x^2 + a_3 x^3 + \cdots$. (Warning: here the coefficient of x is denoted as a_1, different from the notation used in the last section.) This is equivalent to solve the equation

$$1 + f(x + y + xy) = (1 + f(x))(1 + f(x)).$$

Now

$$\begin{aligned} (1 + f(x))(1 + f(y)) &= (\sum_{n=0}^{\infty} a_n x^n)(\sum_{m=0}^{\infty} a_m x^m) \quad (a_0 = 0 \text{ is understood}) \\ &= \sum_{n,m \geq 0} a_n a_m x^n y^m \end{aligned}$$

and

$$\begin{aligned}1+f(x+y+xy) &= 1+\sum_{n=1}^{\infty} a_n(x+y+xy)^n \\ &= 1+a_1(x+y)+a_2x^2+(a_1+2a_2)xy+a_2y^3+a_3x^3 \\ &\quad +(2a_2+3a_3)x^2y+(2a_2+3a_3)xy^2+a_3y^3+\cdots\end{aligned}$$

Comparing the coefficients of the first several terms, we can see

- $a_1^2 = a_1 + 2a_2$, or equivalently $2a_2 = a_1^2 - a_1$
- $a_2a_1 = 2a_2 + 3a_3$, or equivalently $3a_3 = a_2a_1 - 2a_2$

Therefore, if we work over $\mathbb{Q}$, a_2 is determined by a_1 and a_3 is determined by a_1, a_2. We may guess over $\mathbb{Q}$ all the a_n are inductively determined by a_1, also notice one shouldn't expect to determine all the a_n from a_1 if we work over F_p. For instance, reduce modulo 3, there's no restriction on the choice of a_3.

The interesting inductive relations listed above arise from the coefficients of xy and xy^2 (also x^2y since x, y are symmetric). This hints us to calculate the coefficients of xy^k.

There are only two possible ways to produce xy^k from the powers of $(x+y+xy)^n$. One is $xy^k = (xy)\cdot y^{k-1}$ from

$$(x+y+xy)^k = kxy^k + \text{other terms},$$

the other is $xy^k = x \cdot y^k$ from

$$(x+y+xy)^{k+1} = (k+1)xy^k + \text{other terms}.$$

Therefore, we have

$$ka_k + (k+1)a_{k+1} = a_1a_k.$$

If we work over $\mathbb{Q}$, then we can write $a_{k+1} = \frac{(a_1-k)a_k}{k+1}$, thus the power series f is completely determined by the choice of a_1. If $a_1 = r \in \mathbb{Q}$, then

$$a_2 = \frac{(r-1)r}{2}, a_3 = \frac{(r-2)(r-1)r}{3\cdot 2}, \ldots, a_k = \binom{r}{k}, \ldots$$

Therefore, the corresponding automorphism is $f_r(x) := (1+x)^r - 1$. (It is not hard to verify f_r is indeed an automorphism of $\mathbb{G}_m$.) For instance, if $r = -1$, then $f_{-1}(x) = (1+x)^{-1} - 1 = -x + x^2 - x^3 + x^4 + \ldots$.

We have thus proven:

Theorem 3.1.

$$\mathbb{Q}^* \to \mathrm{Aut}_{\mathbb{Q}}(\mathbb{G}_m), \quad r \mapsto f_r(x) = (1+x)^r - 1$$

is an isomorphism. Consequently,

$$\mathbb{Z}^* \to \mathrm{Aut}_{\mathbb{Z}}(\mathbb{G}_m), \quad r \mapsto f_n(x) = (1+x)^n - 1$$

is an isomorphism.

Proof. The second statement follows from the first and that a_1 must be some integer n. □

Let's go back to work over $\mathbb{F}_p$. Recall we have

$$(k+1)a_{k+1} = (a_1 - k)a_k$$

so as long as $k+1$ is not divisible by p, a_{k+1} is determined by a_k. The above relation reduced modulo p has a p-periodicity, more precisely we have

- $a_1 =?, a_2 = \binom{a_1}{2}, a_3 = \binom{a_1}{3}, \ldots, a_{p-1} = \binom{a_1}{p-1}$
- $a_p =?, a_{p+1} = \binom{a_1}{2}a_p, a_{p+2} = \binom{a_1}{3}a_p, \ldots, a_{2p-1} = \binom{a_1}{p-1}a_p$
- $a_{2p} =?, a_{2p+1} = \binom{a_1}{2}a_{2p}, \ldots$

Therefore, we see (over $\mathbb{F}_p$)

$$\begin{aligned}1+f(x) &= (1+a_1x+\binom{a_1}{2}x^2+\binom{a_1}{3}x^3+\cdots+\binom{a_1}{p-1}x^{p-1})(1+a_px^p+a_{2p}x^{2p}+\cdots)\\ &= (1+x)^{a_1}(1+a_px^p+a_{2p}x^{2p}+\cdots)\end{aligned}$$

Denote $g(x) = a_px + a_{2p}x^2 + a_{3p}x^3 + \cdots$, then

$$1+f(x) = (1+x)^{a_1}(1+g(x^p)).$$

From $(1+f(x))(1+f(y)) = 1+f(x+y+xy)$ we have

$$(1+x)^{a_1}(1+y)^{a_1}(1+g(x^p))(1+g(y^p)) = (1+x+y+xy)^{a_1}(1+g((x+y+xy)^p))$$

hence $(1+g(x^p))(1+g(y^p)) = 1+g((x+y+xy)^p) = 1+g(x^p+y^p+x^py^p)$.

Denote $x^p = x', y^p = y'$, we thus have

$$(1+g(x'))(1+g(y')) = 1+g(x'+y'+x'y').$$

That is to say, g is an endomorphism of $\mathbb{G}_m$ over $\mathbb{F}_p$. So by the same analysis as before for f,

$$g(x) = (1+x)^{a_p}h(x^p)$$

for some h.

Inductively, we see

$$\begin{aligned}f(x) &= (1+x)^{a_1}(1+x^p)^{a_p}(1+x^{p^2})^{a_{p^2}}\cdots\\ &= \prod_{k=0}^{\infty}(1+x^{p^k})^{a_{k+1}} = \prod_{k=0}^{\infty}(1+x)^{a_{k+1}p^k}\\ &= (1+x)^{\sum_{k=0}^{\infty}a_{k+1}p^k}\end{aligned}$$

Notice that if there's only finitely many nonzero a_k, then $\sum_{k=0}^{\infty}a_{k+1}p^k$ is some integer n and a_{k+1} is the k-th digit of its p-adic representation. The set of the formal sum $\sum_{k=0}^{\infty}a_{k+1}p^k$, where $0 \le a_{k+1} \le p-1$, is precisely the p-adic integers $\mathbb{Z}_p$.

So we have proven:

Theorem 3.2. *The embedding*

$$\mathbb{Z} \to \mathrm{End}_{\mathbb{F}_p}(\mathbb{G}_m), n \mapsto f_n(x) = (1+x)^n - 1$$

naturally extends to an isomorphism

$$\mathbb{Z}_p \simeq \mathrm{End}_{\mathbb{F}_p}(\mathbb{G}_m), n_p = (\cdots a_3a_2a_1)_p \mapsto (1+x)^{a_1}(1+x^p)^{a_2}\cdots - 1.$$

Consequently, $\mathrm{Aut}_{\mathbb{F}_p}(\mathbb{G}_m) \simeq \mathbb{Z}_p^*$.

Let $S\mathrm{Aut}_{\mathbb{F}_p}(\mathbb{G}_m)$ be the subgroup of $\mathrm{Aut}_{\mathbb{F}_p}(\mathbb{G}_m)$ generated by those $f(x) = a_1x + a_2x^2 + \ldots$ with $a_1 = 0$, then we have a split exact sequence

$$0 \to S\mathrm{Aut}_{\mathbb{F}_p}(\mathbb{G}_m) \to \mathrm{Aut}_{\mathbb{F}_p}(\mathbb{G}_m) \xrightarrow{a_1} \mathbb{F}_p^* \to 0$$

Therefore,

$$\mathrm{Aut}_{\mathbb{F}_p}(\mathbb{G}_m) \simeq S\mathrm{Aut}_{\mathbb{F}_p}(\mathbb{G}_m) \oplus \mathbb{F}_p^*$$

Remark 3.3. *In general, given a split exact sequence* $1 \to N \to G \to H \to 1$ *one cannot deduce* $G = N \times H$. *But this is true when the groups are abelian.*

It is also clear from the above analysis that if $a_1 = 0$ then $f(x) = g(x^p)$ and there's no restriction on the coefficients of g, so

$$S\mathrm{Aut}_{\mathbb{F}_p}(\mathbb{G}_m) \simeq \mathrm{End}(\mathbb{G}_m) \simeq \mathbb{Z}_p.$$

We thus recover the well-known isomorphism:

Corollary 3.4.

$$\mathbb{Z}_p^* \simeq \mathbb{Z}_p \oplus \mathbb{Z}/(p-1)$$

As a byproduct, we also have

Proposition 3.5. *For integers* $0 \le k \le n$, *we have*

$$\binom{n}{k} = \binom{a_{l+1}}{b_{l+1}}\binom{a_l}{b_l}\cdots\binom{a_1}{b_1} \pmod p$$

where $n = (a_{l+1}\dots a_2a_1)_p, k = (b_{l+1}\dots b_2b_1)_p$ *are the p-adic representations of* n, k.

Proof. Over $\mathbb{F}_p$ we have $(1+x)^n = (1+x)^{a_1}(1+x^p)^{a_2}\cdots(1+x^{p^l})^{a_{l+1}}$. □

Corollary 3.6. *Let* n, k *be as in Proposition 3.5, if* $b_i > a_i$ *for some* i, *then* $\binom{n}{k}$ *is divisible by* p.

For instance, if $n = (100\dots0)_p$ is a power of p, then $\binom{n}{k}$ is divisible by p for $0 < k < n$.

4. Steenrod operations and Adams operations

This section assumes certain familiarity with cohomology operations and K-theory.

4.1. $\mathrm{Aut}_{\mathbb{F}_p}(\mathbb{G}_a)$ and Steenrod algebra.

Let p be an odd prime.

Theorem 4.1 (Milnor)**.** *The dual Steenrod algebra is a free commutative graded algebra over* $\mathbb{F}_p$ *generated by even degree elements* $\xi_1, \xi_2, \xi_3, \dots$ *and odd degree elements* $\tau_0, \tau_1, \tau_2, \dots$. *Moreover, it is a Hopf algebra whose co-multiplication* Δ *is given by*

$$\Delta\xi_k = \sum_{i=0}^{k} \xi_{k-i}^{p^i} \otimes \xi_i, \quad \Delta\tau_k = \tau_k \otimes 1 + \sum_{i=0}^{k} \xi_{k-i}^{p^i} \otimes \tau_i$$

and anti-automorphism c *is given by*

$$\sum_{i=0}^{k} \xi_{k-i}^{p^i} \cdot c(\xi_i) = 0, \quad \tau_k + \sum_{i=0}^{k} \xi_{k-i}^{p^i} \cdot c(\tau_i) = 0.$$

Theorem 4.2. *The dual Steenrod algebra modulo can be naturally identified with the coordinate ring of the tangent bundle of* $\mathrm{Aut}_{\mathbb{F}_p}(\mathbb{G}_a)$ *restricted to* $S\mathrm{Aut}_{\mathbb{F}_p}(\mathbb{G}_a)$.

Sketch of proof. This follows immediately from Proposition 2.2 and the observation that $d\xi_k$ behaves the same as τ_k. □

Remark 4.3. *I think the statement of Theorem 4.2 can be improved, for instance degree of* ξ_k *is not discussed yet. The appropriate way is to view* ξ_k *as coordinate of a weighted projective space and then* $\xi_0 = 1$ *is an affine chart. There's certainly more to say.*

4.2. $\mathrm{Aut}_{\mathbb{F}_p}(\mathbb{G}_m)$ **and Adams operations.** Recall that Adams operations Ψ^n are natural (as in topology with respect to continuous maps) ring homomorphisms characterized by

- Ψ^n(line bundle η) $= \eta^n = \eta \otimes \eta \otimes \cdots \otimes \eta$ (n-times). It follows Ψ^n acts on $K(\mathbb{C}P^\infty) = \mathbb{Z}[x]$ as $\Psi^n(x) = (1+x)^n - 1$.
- $\Psi^n \circ \Psi^m = \Psi^{nm}$

It directly follows from Theorem 3.2 that,

Theorem 4.4. *The Adams operations on p-completed K-theory can be naturally identified with* $\mathrm{End}_{\mathbb{F}_p}(\mathbb{G}_m)$.