PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 80, Number 2, October 1980

POLYNOMIAL GROUP LAWS. II

ZENSHO NAKAO

ABSTRACT. Let V be a Zariski-open (i.e., cofinite) subset of an infinite field K. Call a map $m: V \times V \to V$ separately polynomial if for each $x \in V$ the two partial maps $y \to m(x, y)$, $y \to m(y, x)$ are polynomial. If $m: V \times V \to V$ is a separately polynomial group law, then either $V = K$ and $m(x, y) = x + y + k$ for some $k \in K$ or $V = K - \{k\}$ and $m(x, y) = b(x - k)(y - k) + k$ for some $k \in K$ and $b \in K^* = K - \{0\}$.

Let V be a Zariski-open subset of an infinite field K. Then V is of the form $V = K - S$, where S is a finite set. Following [**P**], we call a map $m: V \times V \to V$ separately polynomial if for each $x \in V$ the two partial maps $y \to m(x, y)$, $y \to m(y, x)$ are polynomial. (See also [**M**], [**N1**], [**N2**].)

The objectives of this paper are (1) to determine when a Zariski-open V will admit a group law $m(x, y)$ which is also separately polynomial and (2) to obtain an explicit formula for $m(x, y)$ whenever it exists.

THEOREM. *If $m: V \times V \to V$ is a separately polynomial group law, then either $V = K$ (i.e., $S = \varnothing$) and $m(x, y) = x + y + k$ for some $k \in K$, or $V = K - \{k\}$ (i.e., $S = \{k\}$) for some $k \in K$ and $m(x, y) = b(x - k)(y - k) + k$ for some $b \in K^* = K - \{0\}$.*

We considered the case $V = K$ in [**N2**]. The theorem states as we will see in the subsequent demonstration, that it is impossible to furnish $V = K - \{k_1, \ldots, k_n\}$ with a polynomial group structure when $n \geqslant 2$. We will prove the theorem in several steps.

PROOF. *Step* 1. $S = \varnothing$ (i.e., $V = K$). For completeness we will present an entire proof for the step, although it is given in [**N2**]. Write $m(x, y) = x^*y$ and define $L_x(y) = x^*y = R_y(x)$. Then by assumption L_x and R_x are polynomial maps $K \to K$ for each $x \in K$. Now if P and Q are polynomial bijections $K \to K$ such that $P(Q(z)) = z$ for all $z \in K$ then clearly P and Q have degree one. (Here is where we need K infinite, to guarantee that a polynomial is determined by its values at points of K.) Applying this to L_x and $L_{(x^{-1})}$ (and to R_x and $R_{(x^{-1})}$) we see that $L_x(y) = B(x)y + A(x) = R_y(x) = D(y)x + E(y)$ where A, B, D and E are polynomials of degree at most one, and B and D are nonzero everywhere. It follows, of course, that B and D are nonzero constants b' and d', while $A(x) = ax + a'$ and $E(y) = ey + e'$. Clearly $a = d'$, $e = b'$ and $a' = e'$, so $x^*y = ax + b'y + a'$ for $a, b' \in K^*$

Received by the editors July 18, 1979; presented to the Society, June 15, 1979.
1980 *Mathematics Subject Classification*. Primary 12E10, 14E05; Secondary 14L10.
Key words and phrases. Separately polynomial group laws.

0002-9939/80/0000-0501/$02.25

and $a' \in K$. Finally the associativity of the group law yields $a^2 = a$ and $b'^2 = b'$, so $a = b' = 1$. Hence $m(x, y) = x^*y = x + y + a'$.

Step 2. $S = \{k\}$ (so $V = K - \{k\}$). Write as before $m(x, y) = x^*y$ and define L_x, R_x, A, B, D and E where A, B, D and E are polynomials of degree at most one, and B and D are nonzero now on V.

Although we can argue directly we will consider first the special case $k = 0$ since the later generalization becomes easier this way; so $V = K^*$. Let $B(x) = bx + b'$ and $D(y) = dy + d'$. Then from the identity $L_x(y) = R_y(x)$ we get $b = d$, $a = d'$, $b' = e$ and $a' = e'$. There are two possible cases.

(i) $b\ (= d) = 0$, $b'\ (= e) \neq 0$ and $d'\ (= a) \neq 0$. As in Step 1 we can write $x^*y = b'y + ax + a'$ and, by the associativity of the group law, we obtain $a = b' = 1$; so $x^*y = x + y + a'$. We will show that the group closure axiom is not satisfied on V. Since K is an infinite field we can find infinitely many solutions of the equation $x^*y = x + y + a' = 0$ with $x \neq 0$ and $y \neq 0$, i.e., $(x, y) \in V \times V$. Hence the formula for x^*y cannot be a group multiplication.

(ii) $b\ (= d) \neq 0$. Even though $B(x)$ and $D(y)$ cannot take zero on V, $B(x) = 0$ when $x = -b'/b$ and $D(y) = 0$ when $y = -d'/d$; so we must have $-b'/b = -d'/d = 0\ (\notin V)$, i.e., $b' = d' = 0$. Hence we may put $x^*y = bxy + a'$ for $b \in K^*$ and $a' \in K$. But the associativity of the group law yields $a' = 0$. Therefore, $x^*y = bxy$. We can easily show that the identity element is $1/b$ and the inverse of x is given by $x^{-1} = 1/(b^2x)$. Of course the formula $x^*y = bxy$ is a special case of $x^*y = b(x - k)(y - k) + k$ for $k \in K$; hence the formula $x^*y = bxy$ is the only polynomial group multiplication on V.

Now we consider the more general case $V = K - \{k\}$, where $k \in K$. Define a polynomial bijection f: $K^* \to V$ by $f(x) = x + k$. Then the inverse function is given by $f^{-1}(x) = x - k$, which is also polynomial, and, therefore, we can transport the polynomial group structure of V to K^* via f by $x^*y = f^{-1}[m(f(x), f(y))]$ for $x, y \in K^*$, where m: $V \times V \to V$ is the given polynomial group law. But the only polynomial group structure on K^* is given by $x^*y = bxy$ for some $b \in K^*$ as we saw in the special case $V = K^*$. By rewriting the group multiplication we obtain

$$\begin{aligned} m(x, y) &= f\big[f^{-1}(x)^*f^{-1}(y)\big] = f\big[(x - k)^*(y - k)\big] \\ &= f\big[b(x - k)(y - k)\big] = b(x - k)(y - k) + k, \end{aligned}$$

which was to be shown.

Step 3. $S = \{k_1, k_2\}$ (so $V = K - \{k_1, k_2\}$). We first assume that $S = \{0, 1\}$ extending the special case in Step 2, and show that $V = K - S$ cannot carry a polynomial group law.

(i) $b\ (= d) = 0$. As in (i) of Step 2, we can write $x^*y = x + y + a'$. However, we can find infinitely many $(x, y) \in K \times K$ such that $x + y + a' = 0$ since K is an infinite field, so we can choose some $(x, y) \in V \times V$ with $x + y + a' = 0\ (\notin V)$, violating the closure axiom. Hence the formula $x^*y = x + y + a'$ cannot define a polynomial group law on V.

(ii) $b\ (= d) \neq 0$. Extending (ii) of Step 2, we can get $-b'/b = 0$ or $-b'/b = 1$,

and $-d'/d = 0$ or $-d'/d = 1$; so $b' = 0$ or $b + b' = 0$, and $d' = 0$ or $d + d' = 0$. Then there are four possible cases.

(a) $b' = 0$ and $d' = 0$. From $L_x(y) = R_y(x)$, we can obtain $x^*y = bxy + a'$ and the associativity of the group law gives $a' = 0$. Hence $x^*y = bxy$, for $b \in K^*$. Evidently, as before, the identity element is $1/b$, and therefore we require $b \neq 1$ in order to have $1/b \in V$. The inverse of x is $x^{-1} = 1/(b^2x)$, so we must have $1/(b^2x) \neq 1$ for all $x \neq 0, 1$. But the equation $1/(b^2x) = 1$ has a unique solution $x = 1/b^2$, and if $b^2 \neq 1$ then $x = 1/b^2 \in V$ and $x^{-1} = 1 \notin V$. This means that we must have $b^2 = 1$, and hence $b = -1$ since $b \neq 1$. Therefore $x^*y = -xy$. However, there are infinitely many pairs $(x, y) \in V \times V$ such that $-xy = 1$ $(\notin V)$, so $x^*y = -xy$ cannot satisfy the closure axiom.

(b) $b' = 0$ and $d + d' = 0$. We can derive $x^*y = bxy - bx + a'$ from $L_x(y) = R_y(x)$. But the associativity of the group law gives $b^2 = 0$, and therefore $b = 0$, which is a contradiction. So this case cannot occur.

(c) $d' = 0$ and $b + b' = 0$. This case is also impossible for a reason similar to that for (b).

(d) $b + b' = 0$ and $d + d' = 0$ (and thus $b' \neq 0$ and $d' \neq 0$). First we can derive $x^*y = bxy - bx - by + a'$, and then, by the associativity of the group law, we can get $a' = 1 + b$; so we obtain $x^*y = b(x - 1)(y - 1) + 1$. The identity element is $1 + 1/b$, so we need to have $b \neq -1$ in order to satisfy $1 + 1/b \neq 0$. The inverse of x is $x^{-1} = 1 + 1/[b^2(x - 1)]$. Clearly $x^{-1} \neq 1$. But the equation

$$1 + 1/\left[b^2(x - 1)\right] = 0$$

has a unique solution $x = 1 - 1/b^2$, and if $1 - 1/b^2 \neq 0$ then $x = 1 - 1/b^2 \in V$ and $x^{-1} = 0 \notin V$. So we must require further that $1 - 1/b^2 = 0$, i.e., $b^2 - 1 = 0$. Since $b \neq -1$, we have only one choice, $b = 1$. Hence $x^*y = (x - 1)(y - 1) + 1$. However, as in case (ii)(a), we can find some $(x, y) \in V \times V$ such that $(x - 1)(y - 1) + 1 = 0$ because K is an infinite field, so $x^*y = (x - 1)(y - 1) + 1$ cannot satisfy the closure axiom.

Now we will go back to the general case $V = K - \{k_1, k_2\}$. Define a polynomial bijection f: $K - \{0, 1\} \to V$ by $f(x) = (k_2 - k_1)x + k_1$ which satisfies $f(0) = k_1$ and $f(1) = k_2$. Then $f^{-1}(x) = (x - k_1)/(k_2 - k_1)$ is also polynomial.

If v does possess a polynomial group structure m, then we can define a polynomial group structure $*$ on $K - \{0, 1\}$ also via f by $x^*y = f^{-1}[m(f(x), f(y))]$ for $x, y \in K - \{0, 1\}$, which contradicts what we have found about $K - \{0, 1\}$. Hence V cannot carry a polynomial group structure.

Step 4. $S = \{k_1, k_2, \ldots, k_n\}$ (so $V = K - \{k_1, k_2, \ldots, k_n\}$), $n > 2$. Define a polynomial bijection f: $K \to K$ by $f(x) = (k_2 - k_1)x + k_1$, which satisfies $f(0) = k_1$ and $f(1) = k_2$. Let $k_i' = f^{-1}(k_i)$, $3 \leqslant i \leqslant n$, or more explicitly,

$$k_i' = (k_i - k_1)/(k_2 - k_1),$$

and let $T = \{0, 1, k_3', \ldots, k_n'\}$. We will first show that $V = K - T$ cannot be given a polynomial group structure, generalizing the argument used in Step 3.

(i) $b\ (=d)=0$. As before we may write $x^*y=x+y+a'$. Given a', there are infinitely many pairs $(x,y)\in K\times K$ with $x+y+a'=0$ and we can certainly avoid $x,\ y\in\{0,\ 1,\ k_3',\ \ldots,\ k_n'\}$. So with such a pair $(x,y)\in V\times V$, we have $x^*y=x+y+a'=0\notin V$; i.e., the closure axiom is not satisfied.

(ii) $b\ (=d)\neq 0$. Further extending (ii) of Step 3, we can get $-b'/b=0$, $-b'/b=1$, $-b'/b=k_3',\ \ldots,$ or $-b'/b=k_n'$, and $-d'/d=0$, $-d'/d=1$, $-d'/d=k_3',\ \ldots,$ or $-d'/d=k_n'$. So $b'=0$, $b+b'=0$, $b'+bk_3'=0,\ \ldots,$ or $b'+bk_n'$, and $d'=0$, $d+d'=0$, $d'+dk_3'=0,\ \ldots,$ or $d'+dk_n'$. Due to the symmetry of the role of b and d, it suffices to consider the following six cases.

(a) $b'=0$ and $d'=0$. Just as in case (ii)(a) of Step 3, the group law is given by $x^*y=bxy$, for some $b\in K^*$ and since there are some $(x,y)\in V\times V$ such that $bxy=1\notin V$ (again because K is an infinite field), the formula for x^*y cannot satisfy the closure axiom.

(b) $b'=0$ and $d+d'=0$. The case is identical to case (ii)(b) of Step 3; so a possible formula for the group multiplication is $x^*y=bxy-bx+a'$, and the associativity of the group law requires $b^2=0$, hence, $b=0$, which is a contradiction. So this case cannot happen.

(c) $b'+b=0$ and $d+d'=0$ (and therefore $b'\neq 0$ and $d'\neq 0$). The case corresponds to (ii)(d) of Step 3; so a possible formula for the group law is $x^*y=bxy-bx-by+a'$. But the associativity of the group law requires $a'=1+b$, so we derive $x^*y=b(x-1)(y-1)+1$. However, we can find some pairs $(x,y)\in V\times V$ such that $b(x-1)(y-1)+1=0$ since K is an infinite field, so again the formula for x^*y does not satisfy the closure axiom.

(d) $b'=0$ and $d'+dk_m'=0$ for some $m=3,\ \ldots,\ n$. First we can derive $x^*y=bxy-bk_m'x+a'$ from $L_x(y)=R_y(x)$, the $b^2k_m'=0$ from the associativity of the group multiplication; so $k_m'=0$ because $b\neq 0$, which is a contradiction since $k_m'\neq 0,\ 1$ for any $m=3,\ \ldots,\ n$. Hence there cannot be a group law on V.

(e) $b'+b=0$ and $d'+dk_m'=0$ for some $m=3,\ \ldots,\ n$. Reasoning as in the case (d) above, we find that a possible group multiplication is $x^*y=bxy-bk_m'x-by+a'$ and the associativity of the multiplication gives $b^2k_m'=b^2$, so $k_m'=1$ because $b\neq 0$, which is again a contradiction since $k_m'\neq 0,\ 1$ for any $m=3,\ \ldots,\ n$. Hence V cannot carry a group law.

(f) $b'+bk_m'=0$ and $d'+dk_p'=0$ for some $m,\ p=3,\ \ldots,\ n$, and it is possible that $m=p$. From $L_x(y)=R_y(x)$ we get $x^*y=bxy-bk_p'x-bk_m'y+a'$, and the associativity implies $k_m'=k_p'$, and $a'b=b^2k_m'^2+bk_m'$ so $a'=bk_m'^2+k_m'$. Rewriting the multiplication we obtain $x^*y=b(x-k_m')(y-k_m')+k_m'$. This possible formula for the group law cannot satisfy the closure axiom. There are some $(x,y)\in V\times V$ such that $b(x-k_m')(y-k_m')+k_m'=0$ because K is an infinite field, so $x^*y=0\notin V$. Hence the multiplication x^*y cannot satisfy the closure axiom.

Summarizing all cases considered, we found that $V=K-T=K-\{0,\ 1,\ k_3',\ \ldots,\ k_n'\}$ cannot be given a polynomial group structure. Now we will examine the general case $V=K-\{k_1,\ k_2,\ \ldots,\ k_n\}$. The polynomial bijection $f\colon K\to K$ defined at the beginning of Step 4 is evidently a bijection from $K-T$ onto V. So if V does have a polynomial group law m then we can transfer the structure to $K-T$

via f by $x^*y = f^{-1}[m(f(x), f(y))]$ for all $x, y \in K - T$. But we showed that $K - T$ cannot be given a polynomial group structure, hence V cannot either.

This completes the proof of the theorem.

References

[M] A. R. Magid, *Separately algebraic group laws*, Amer. J. Math. **100** (1978), 407–409.

[N1] Z. Nakao, *Bi-algebraic groups*, J. Algebra **57** (1979), 1–9.

[N2] _____, *Polynomial group laws*, Amer. Math. Monthly (to appear).

[P] R. Palais, *Some analogues of Hartogs' Theorem in an algebraic setting*, Amer. J. Math. **100** (1978), 387–405.

Department of Mathematics, Southern Illinois University, Carbondale, Illinois 62901

Current address: Department of Mathematical Sciences, University of Wisconsin, Milwaukee, Wisconsin 53201