TAMKANG JOURNAL OF MATHEMATICS
Volume 37, Number 4, 297-299, Winter 2006

# A NOTE ON THE LIE POLYNOMIAL $(x+y)^p - x^p - y^p$

RONGZHENG JIAO

**Abstract**. Using the techniques of group action on a set, we will give an elementary ane complete proof in this paper that the Lie polynomial $(x+y)^p - x^p - y^p$ over prime field $F_p$ is a sum of Lie brackets, with $p$ a rational prime.

## 1. Introduction

Let's introduce some notations first. Let $F_p$ be a prime field with $p$ elements, and $x$, $y$ be two letters. We form the associative (but not commutative) formal series $F_p[[x,y]]$ free generated by these two letters with coefficients in $F_p$. For any series with only finite non-zero terms will be called Lie polynomial. For a Lie polynomial we can define the degree of $x$ and $y$ and total degree respectively as the usual polynomial, but remember $xy \neq yx$. We only concern the Lie polynomial $(x+y)^p - x^p - y^p$ and its homogenous part in this note. And the Lie brackets $[,]$ is a bilinear map defined on every associative algbra R as $[A,B] = AB - BA$, for any $A \in R$, $B \in R$ so that the associative algebra R becomes a Lie algebra. For more details about Lie algebra please consult any standarded textbook on it, and we will not use these in this note.

There are many seminars with the aim to work through professor Michel Lazard's thesis [4]. And such as the seminar held at Oxford in 1989 came out a book [2]. In this very important paper, professor Michel Lazard mentioned that the Lie polynomial $(x+y)^p - x^p - y^p$ is a sum of Lie brackets. He said that this is an identity of Jacobson in [3] char.V section 7. But the identity in [3] only given in for $p = 2, 3$ and 5. For general $p$ we can not find the proof in the references we can get, such as Bourbaki [1] and other textbooks on Lie algebra.

The aim of this note is to give a elementary and complete proof of this claim.

**Theorem.** *Let $p$ be a rational prime, the Lie polynomial $(x+y)^p - x^p - y^p$ is a sum of Lie brackets over $F_p$.*

Received March 2, 2005.
2000 *Mathematics Subject Classification.* 17B70, 16W22.
*Key words and phrases.* Lie polynomial, Lie bracket, group actions, finite field.
The author would like to thank the financial supported from China Scholarship Council for his visiting to Department of Mathematics of the University of West Ontario. This work is finished during a seminar presided by prof. John Labute and prof. Jan Minac. The author would like to thank these two professors as well as Dr. Ganesh Abhandari for many useful discussions with them. This work is also partly supported by NSFC project 10471121.

## 2. Proof of the Theorem

For any fixed integer $k_0$, with $1 \leq k_0 \leq p-1$, put the set

$$M_{k_0} = \{X_1 X_2 \cdots X_p : \text{where } X_j = x \text{ or } y,$$

$$\text{and there are } k_0\, x \text{and } p-k_0\, y \text{in this associative product}\},$$

i.e. this is just the set of all mononials with the degree $k_0$ of $x$, the degree $p-k_0$ of $y$ and the total degree $p$. Please note that the cardinal $|M_{k_0}|$ of $M_{k_0}$ is $\binom{p}{k_0}$, and it is divisible by $p$. We define a map from $(G, M_{k_0})$ to $M_{k_0}$ as following, where $G = \{T_1, T_2, \cdots T_p\}$.

$$\begin{aligned} &T_i(X_1 X_2 \cdots X_{i-1} X_i \cdots X_p) \\ &= X_i X_{i+1} \cdots X_p X_1 X_2 \cdots X_{i-1}, \text{for any } X_1 X_2 \cdots X_{i-1} X_i \cdots X_p \in M_{k_0}. \end{aligned}$$

We know from this definition that the image of any element in $M_{k_0}$ under $T_i$ is still in $M_{k_0}$. This operation is a bit similar to the parall translation and mirror reflection in Euclid plane geometry. And we define an operation in $G$ as the composite of maps. Thus we can see that $G$ becomes an group under this operation. As this group $G$ is isomorphic to additive group of $(F_p, +)$. Note that the map we have just defined from $(G, M_{k_0})$ to $M_{k_0}$ is really an group action of $G$ on $M_{k_0}$. For any $m \in M_{k_0}$, we form the orbit $O_m = \{T_i m : 1 \leq i \leq p\}$ under the action of $G$. The above notions can be found in any standard group theory textbook. Let's recall a wellknown fact from group theory that the set $M_{k_0}$ with the group $G$ action on it can be divided as a disjoint union of different union of orbits $O_m$, $m$ through $M_{k_0}$; the orbit $O_m$ has $|G/stab_m|$ element(s), where $stab_m = \{g \in G : gm = m\}$ the stablizer of $m$. And we know that $|G| = p$, so $|G/stab_m| = 1 \,\text{or}\, p$. But a simple calculation show that $stab_m = G$ only if $m = x^p \,\text{or}\, y^p$. That is for $m \in M_{k_0}, 1 \leq k_0 \leq p-1$, $|G/stab_m| = p$. Note that

$$\begin{aligned} &T_i(X_1 X_2 \cdots X_{i-1} X_i \cdots X_p) - X_1 X_2 \cdots X_{i-1} X_i \cdots X_p \\ &= [X_i X_{i+1} \cdots X_p, X_1 X_2 \cdots X_{i-1}]. \end{aligned}$$

So any two elements in a same orbit different by a sum of Lie bracket(s), and the sum of all elements in a given orbit is a sum of Lie brackets over $F_p$, for in total there are $p$ elements in the orbit.

with all these preparation, we come to the proof of the theorem.

$$(x+y)^p - x^p - y^p = \sum_{k_0=1}^{p-1} \sum_{m \in M_{k_0}} m,$$

and we divide $\sum_{m \in M_{k_0}} m$ into a finite sum of the sum of elements in a orbit, with proceeding remark, we get the proof of the theorem.

## References

[1] N. Bourbaki, Lie Groups and Lie Algebra, Part I, Hermann, Paris, 1975.
[2] J. D. Dixon, M. P. F. du Sautoy, A. Mann and D. Segal, Analytic Pro-$p$ Groups, Cambridge University Press, Cambridge, 1991.
[3] N. Jacobson, Lie Algebras, John Wiley and Sons, INC, 1962.
[4] M. Lazard, *Groupes analytiques $p$-adiques*, IHES., Publ. Math. **26**(1965), 389-603.

Department of Mathematics, Yangzhou University, Yangzhou, Jiangsu, 225002, P. R. China.
E-mail: rzjiao@hotmail.com