www.theoryofgroups.ir

International Journal of Group Theory
ISSN (print): 2251-7650, ISSN (on-line): 2251-7669
Vol. x No. x (201x), pp. xx-xx.

www.ui.ac.ir

HILBERT'S THEOREM 90 FOR FINITE NILPOTENT GROUPS

WILLIAM COCKE

Communicated by Gustavo Adolfo Fernndez-Alcober

Abstract. In this note we prove an analog of Hilbert's theorem 90 for finite nilpotent groups. Our version of Hilbert's theorem 90 was inspired by the Boston–Bush–Hajir (BBH) heuristics in number theory and will be useful in extending the BBH heuristics beyond quadratic field extensions.

1. Introduction.

Hilbert's theorem 90 is a famous result in Galois theory. The fame of the original result has eclipsed a more general result due to Noether and often references to Hilbert's theorem 90 are actually references to Noether's generalization of Theorem 90. For our purposes Hilbert's theorem 90 is the statement below.

Theorem 1.1 (Hilbert's Theorem 90)**.** *Let K be a field and let L be a field extension of K such that $G := Gal(L/K)$ is cyclic of order n and generated by an element σ. If $a \in L$ satisfies*

$$N_{L/K}(a) = \prod_{i=1}^{n} \sigma^i(a) = 1,$$

then there is some $b \in L$ such that $a = b^{-1}\sigma(b)$.

MSC(2010): Primary: 20D15; Secondary: 20F18.
Keywords: Nilpotent groups, BBH Heuristics, Hilbert's Theorem 90.
Received: 04 April 2019, Accepted: 13 August 2019.

http://dx.doi.org/10.22108/ijgt.2019.116275.1545

.

Recall that $N_{L/K}$ is a norm function, inspired by the norm function over the complex numbers. Since automorphisms preserve norms, it is not hard to see that

$$N_{L/K}(b^{-1}\sigma(b)) = 1.$$

Hilbert's Theorem 90 is equivalent to the statement that the sets

$$X = \{x \in L : \prod_{i=1}^{n} \sigma^i(x) = 1\}$$

and

$$Y := \{y^{-1}\sigma(y) : y \in L^*\}$$

are equal.

Due to its importance within Galois theory, there have been many attempts to extend Hilbert's theorem 90 to different algebraic structures. We mention the recent work of Quadrelli and Weigel in group theory [3]. In this note we present a novel analog of Hilbert's theorem 90 to nilpotent groups. Our motivation for doing so comes from number theory and the Boston–Bush–Hajir heuristics [1]. Throughout the paper we will reserve the symbol p for a prime number. The BBH heuristics involve the proportion of field extensions of a certain type whose p-class tower group is isomorphic to some fixed p-group G. The defining relations of G are described by sets analogous to the above X and Y. In these cases the equality of the two sets allows one to more readily prove results about the underlying structure. The theorem below will be useful in generalizing the BBH heuristics beyond quadratic field extensions.

Theorem A. *Let G be a finite nilpotent group and let $\sigma \in Aut(G)$ have order n that is coprime to the order of G. Then the sets*

$$X = \{x \in G : \prod_{i=1}^{n} \sigma^i(x) = 1\}$$

and

$$Y := \{y^{-1}\sigma(y) : y \in G\}$$

are equal.

Note that since in general G is nonabelian,

$$\prod_{i=1}^{n} \sigma^i(x) = \sigma(x)\sigma^2(x)\cdots\sigma^n(x),$$

and the order of the product matters.

In the proof we will show that the map $X \to Y$ given by sending x to $x^{-1}\sigma(x)$ is an injection of sets. The restriction to nilpotent groups allows us to provide an exceptionally clean proof.

DOI: http://dx.doi.org/10.22108/ijgt.2019.116275.1545

2. **Proof of Theorem.**

We will need the following technical lemma.

Lemma 2.1. *Let G be a finite nilpotent group and let $\sigma \in Aut(G)$ have order n that is coprime to the order of G. Let*

$$X(G) = \{x \in G : \prod_{i=1}^{n} \sigma^i(x) = 1\}.$$

If for some g and h in $X(G)$ we have that $g = kh$ where $\sigma(k) = k$, then $k = 1$.

Proof. Suppose G is abelian. If for $g, h \in X(G)$ we have that $g = kh$ where $\sigma(k) = k$, then

$$\prod_{i=1}^{n} \sigma^i(g) = \prod_{i=1}^{n} \sigma^i(kh) = k^n \underbrace{\prod_{i=1}^{n} \sigma^i(h)}_{1} = k^n.$$

Because $g \in X(G)$ we see that $k^n = 1$. Since n is coprime to the order of G, we see that $k = 1$.

Now suppose that G is a finite nilpotent group, but not abelian. We will proceed by induction on the order of G. Suppose that for all nilpotent groups with order less than the order of G, the lemma holds; i.e., if $|H| < |G|$, then if for two elements $a, b \in X(H)$ we have that $a = cb$ where $\sigma(c) = c$, then $c = 1$. Returning to G, suppose we have g and h in $X(G)$ with $g = kh$. Let $Z = \mathbf{Z}(G)$ and consider the quotient G/Z. Since G is nilpotent and nonabelian, $1 < Z < G$ and $\overline{G} = G/Z$ satisfies $|\overline{G}| < |G|$. Since Z is a characteristic subgroup of G we know that there is an automorphism $\overline{\sigma} \in Aut(G/Z)$ such that $\overline{\sigma}(\overline{g}) = \overline{\sigma(g)}$. Moreover, $\overline{g}$ and $\overline{h}$ are in

$$X(\overline{G}) = \{\overline{x} \in \overline{G} : \prod_{i=1}^{n} \sigma^i(\overline{x}) = \overline{1}\}.$$

By the inductive hypothesis we conclude that $\overline{k} = \overline{1}$, i.e., that $k \in Z$. As in the abelian case we have

$$\prod_{i=1}^{n} \sigma^i(g) = \prod_{i=1}^{n} \sigma^i(kh) = k^n \underbrace{\prod_{i=1}^{n} \sigma^i(h)}_{1} = k^n = 1.$$

Since n is coprime to the order of G, we see that $k = 1$. □

We can now prove Theorem A.

Proof of Theorem A. We note that $Y \subseteq X$. We will show that $|Y| = |X|$ and hence that $Y = X$. Consider the set map $f : G \to Y$, where $f(x) = x^{-1}\sigma(x)$. If $f(g) = f(h)$, then

$$g^{-1}\sigma(g) = h^{-1}\sigma(h) \tag{2.1}$$

$$hg^{-1}\sigma(g)\sigma(h^{-1}) = 1 \tag{2.2}$$

$$f(gh^{-1}) = 1. \tag{2.3}$$

Note that $f(gh^{-1}) = 1$ if and only if $\sigma(gh^{-1}) = gh^{-1}$.

DOI: http://dx.doi.org/10.22108/ijgt.2019.116275.1545

Now suppose that for g and h in X we have that $f(g) = f(h)$. Then $g = (gh^{-1})h$ and by the above lemma, we conclude that $gh^{-1} = 1$. So f is injective from X to Y and therefore $X = Y$. □

We reiterate that Theorem A was originally motivated by number theory, but the simple and elegant proof make it interesting in its own right. The function f is a type of crossed homomorphism in that $f(xy) = y^{-1}f(x)yf(y)$. The interested reader can learn more about crossed homomorphisms in [2].

Acknowledgments

This material is based upon work done while the first author was supported by the National Science Foundation under Grant No. DMS-1502553. Some of the work was done while the first author was visiting the Army Cyber Institute. The views expressed are those of the author and do not reflect the official policy or position of the Army Cyber Institute, West Point, the Department of the Army, the Department of Defense, or the US Government.

References

[1] N. Boston, M. R. Bush and F. Hajir, Heuristics for p-class towers of imaginary quadratic fields, *Math. Annalen.*, **368** (2017) 633–669.

[2] I. M. Isaacs, *Finite Group Theory*, Graduate Studies in Mathematics, **92**, Providence, RI: American Mathematical Society, 2008.

[3] C. Quadrelli and T. Weigel, A group-theoretical version of Hilbert's theorem 90, *Bull. London Math. Soc.*, **47** (2015) 704–714.

William Cocke

Department of Mathematics, University of Wisconsin Madison, WI, USA

Email:cocke@math.wisc.edu

DOI: http://dx.doi.org/10.22108/ijgt.2019.116275.1545