ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 17, Number 4, Fall 1987

SOLUTIONS OF EQUATIONS OVER ω–NILPOTENT GROUPS

S.M. GERSTEN

While studying the general question of solving equations in groups, I came across the curious fact the Newton's algorithm applies in a variety of noncommutative situations. In particular, if G is an ω–nilpotent group and $w \in G * \langle t \rangle$ is an equation with exponent sum $e_t(w) = \pm 1$, then $w(t) = 1$ has a unique solution in $U_1(\mathbf{Z}[G]\hat{})$. Here $\mathbf{Z}[G]\hat{}$ is the completion of the integral group ring $\mathbf{Z}[G]$ in the I_G–adic topology, I_G the augmentation ideal, and U_1 refers to units $\equiv 1 \bmod I_G\hat{}$.

More generally, let A be a ring equipped with a descending filtration $\{\sigma_n\}$ of two sided ideals (so $\sigma_0 = A, \sigma_i \cdot \sigma_j \subseteq \sigma_{i+j}$). Assume A is complete–i.e. the canonical map $A \to \varprojlim_n A/\sigma_n$ is an isomorphism. Let $U_1(A)$ denote the group of units of A congruent to 1 modulo σ_1. Let $w \in U_1(A) * \langle t \rangle$ be such that $e_t(w)$ is a unit in A. Then the equation $w(t) = 1$ has a unique solution in $U_1(A)$.

Applied to $\mathbf{Q}G$, where G is *fg* torsion free nilpotent, this implies the classical result that $U_1(\mathbf{Q}G\hat{})$ contains the Mal'cev completion [**2**] of G.

A quick homological proof is offered of the Kervaire conjecture for ω–nilpotent groups. I am aware there are other proofs based on residual properties. With that out of the way, the proper topic of this paper, uniqueness of solutions, can begin.

This work was done while I was on sabbatical leave from the University of Utah.

1. Existence of solutions. Let G be a group, $G\langle t \rangle$ the free product of G with an infinite cycle $\langle t \rangle$, and $w(t) \in G\langle t \rangle$. Let $e_t(w)$ be the exponent sum of t in $w(t)$. The Kervaire conjecture is that G injects in $G\langle t \rangle / N$, where N is the normal closure of $w(t)$ in $G\langle t \rangle$, provided $e_t(w) = \pm 1$. This is equivalent to the existence of a group G_1 containing G as a subgroup and an element $x \in G_1$ such that $w(x) = 1$.

Let $\Gamma_n(G)$ denote the lower central series of a group G; thus $\Gamma_0(G) = G$ and $\Gamma_{n+1}(G) = (G, \Gamma_n(G))$. Similarly, if p is a prime number, let $\Gamma_{n,p}(G)$ be the p–lower central series; thus $\Gamma_{o,p}(G) = G$ and $\Gamma_{n+1,p}(G)$

Received by the editors on September 24, 1982.

is generated by all commutators $[g, x]$ and x^p, where $g \in G, x \in \Gamma_{n,p}(G)$.

THEOREM 1.1. *Let $w \in G\langle t\rangle$ and let K be the kernel of the map $G \to G\langle t\rangle/N$, where N is the normal closure of w in $G\langle t\rangle$.*

(a) *If $e_t(w) = \pm 1$, then $K \subset \cap_n \Gamma_n(G)$*

(b) *If p is a prime such that $p \nmid e_t(w)$, then $K \subseteq \cap_n \Gamma_{n,p}(G)$.*

PROOF. Let $X = K(G,1)$ be an Eilenberg–MacLane space. Let $Y = X \vee S^1_t \vee_w e^2$, so Y is gotten from the one point union of X with a circle S^1_t (a generator of $\pi_1(S^1)$ has been identified with t) by attaching a 2–cell e^2 via a map $\partial e^2 \to X \vee S^1_t$ representing $w \in \pi_1(X \vee S^1_t) = G\langle t\rangle$. Then $\pi_1(Y) = H =: G\langle t\rangle/N$ by the van Kampen theorem [**4**]. If $e_t(w) = \pm 1$, it follows that $H_*(Y, X) = 0$; so $H.(X) \to H.(Y)$ is an isomorphism. Now $\pi_1(Y) = H = G\langle t\rangle/N$; to construct a $K(H,1)$ from Y, it is necessary to attach r–cells to Y with $r \geq 3$. Let $Z \supseteq Y$ be the $K(H,1)$ so constructed. It follows that $H_i(Y) \to H_i(Z)$ is an isomorphism if $i = 1$ and an epimorphism if $i = 2$. Hence $H_i(G) \to H_i(H)$ is an isomorphism for $i = 1$ and an epimorphism for $i = 2$. It follows [**6**] that $G/\Gamma_n(G) \xrightarrow{\cong} H/\Gamma_n(H)$, all n. In particular, $K \subset \cap_n \Gamma_n G$. The argument for $\Gamma_{n,p}$ is similar, based on the observation that if $p \nmid e_t(w), H.(Y, X; \mathbf{Z}_p) = 0$.

COROLLARY 1.2. *If G is ω–nilpotent and $e_t(w) = \pm 1$, then G imbeds in $H = G\langle t\rangle/N$.*

PROOF. Recall G is said to be ω–nilpotent if $\cap_n \Gamma_n(G) = \{1\}$. The theorem then implies $K = \{1\}$.

REMARK. The same argument applies to systems of equations. We record the result. Let $G\langle t_1, \ldots, t_n\rangle$ be the free product of G with the free group of rank n freely generated by $t_1, \ldots, t_n$. Let $w_1, \ldots, w_n \in G\langle t_1, \ldots, t_n\rangle$ be such that the matrix $M = (e_{t_j}(w_i))$ has determinant d. Let K be the kernel of the map $G \to G\langle t_1, \ldots, t_n\rangle/N$ where N is the normal closure of $w_1, \cdots, w_n$. Then $K \subseteq \cap_n \Gamma_n(G)$ if $d = \pm 1$ and $K \subseteq \cap_n \Gamma_{n,p}(G)$ if p is a prime such that $p \nmid d$.

2. Filtered rings. Let A be an associative ring with unit. A filtration on A is a family of two sided ideals $\sigma_n, n \geq 0$, such that $\sigma_0 = A, \sigma_n \supseteq \sigma_{n+1}$, and $\sigma_i \cdot \sigma_j \subseteq \sigma_{i+j}$. The family of ring homomorphisms $A/\sigma_{n+1} \to A/\sigma_n$ define a map $A \xrightarrow{j} \lim\limits_{\overleftarrow{n}} A/\sigma_n$. We say A is separated if $\operatorname{Ker} j = 0$ and A is complete (with respect to the given filtration) if j is bijective. In any case, $\lim\limits_{\overleftarrow{n}} A/\sigma_n =: A\hat{}$ is a filtered ring, filtered by the family $\sigma\hat{}_m = \lim\limits_{\overleftarrow{n}}(\sigma_m + \sigma_n/\sigma_n)$, and $A\hat{}$ is complete [**1**]. In addition $A/\sigma_n \simeq A\hat{}/\sigma_n\hat{}$ for all n ([**1**; Corollary 10.4]). The kernel of the canonical map $j : A \to A\hat{}$ is $\bigcap_n \sigma_n$.

Suppose now that A is a filtered ring complete with respect to the filtration $\{\sigma_n\}$. Define $U_1(A) = \{x \in A | x \equiv 1 (\operatorname{mod} \sigma_1)\}$. Clearly $U_1(A)$ is closed under multiplication, and if $x = 1 - y \in U_1(A), y \in \sigma_1$, then $x^{-1} = 1 + y + y^2 + \cdots$ converges, so $U_1(A)$ is a group under multiplication.

THEOREM 2.1. *Suppose the filtered ring A is complete. Let $w \in U_1(A) < t >$ be such that $e = e_t(w)$ is a unit in A. Then the equation $w(t) = 1$ has a unique solution in $U_1(A)$.*

PROOF. We shall produce a sequence $x_n \in \sigma_1$ such that
(1) $x_1 = 0$
(2) $w(1 + x_n) \equiv 1 (\operatorname{mod} \sigma_n)$
(3) $x_{n+1} \equiv x_n (\operatorname{mod} \sigma_n)$
If this is done, then the family $\{1 + x_n + \sigma_n \in A/\sigma_n\}$ defines an element $1 + x \in U_1(A)$ which is a solution $w(1 + x) = 1$, and the existence of a solution follows. We need a lemma.

LEMMA 2.2. *Let $x \in \sigma_1, z \in \sigma_n (n \geq 1)$ and let $1 + y = (1 + x)^{-1}$. Then $(1 + x + z)^{-1} \equiv (1 + y - z)(mod \sigma_{n+1})$.*

PROOF. Just compute $(1 + x + z)(1 + y - z)(\operatorname{mod} \sigma_{n+1})$.

The sequence $\{x_n\}$ is constructed by induction with $x_1 = 0$. Observe that $w(1) \equiv 1 (\operatorname{mod} \sigma_1)$ since $w \in U_1(A)\langle t\rangle$, so condition (1) is satisfied. Assume that $x_1, x_2, \ldots, x_m$ have been found such that $x_1 = 0$, (2) is valid for $n < m$ and (3) is valid for $n < m$. Let

$$w(t) = \prod_{i=1}^{r}(1+a_i)t^{\varepsilon_i},$$

$\varepsilon_i = \pm 1, a_i \in \sigma_1, \sum_{i=1}^{r} \varepsilon_i = e$. Let $z \in \sigma_m$, and compute $w(1 + x_m + z)(\operatorname{mod} \sigma_{n+1})$. We see $w(1 + x_m + z) = \prod_{i=1}^{r}(1 + a_i)(1 + x_m + z)^{\varepsilon_i}$

$$\equiv (ez + w(1 + x_m))(\operatorname{mod} \sigma_{m+1}),$$

where Lemma 2.2 was used to evaluate $(1+x_m+z)^{-1}$. But $w(1+x_m) \equiv 1(\operatorname{mod} \sigma_m)$, so write $w(1 + x_m) = 1 - \alpha, \alpha \in \sigma_m$. Now we want z such that $w(1 + x_m + z) \equiv 1(\operatorname{mod} \sigma_{m+1})$ i.e., $ez \equiv \alpha(\operatorname{mod} \sigma_{m+1})$. But e is a unit in A, so $z = e^{-1}\alpha$ is uniquely determined $(\operatorname{mod} \sigma_{m+1})$. Set $x_{m+1} = x_m + e^{-1}\alpha$. Then check (1), (2), (3) when they make sense, and the induction is complete.

Proceeding to uniqueness, we see another solution $w(1+y) = 1$ yields a sequence $\{y_n\}$ of elements in σ_1 satisfying (1), (2), (3). We show by induction on n that $y_n \equiv x_n(\operatorname{mod} \sigma_n)$. This implies $1 + y = 1 + x$ in $A = \lim_{\rightarrow} A/\sigma_n$. Assume then that $x_i \equiv y_i(\operatorname{mod} \sigma_i)$ for $i \leq n$. Then $x_{n+1} \equiv x_n \equiv y_n \equiv y_{n+1}(\operatorname{mod} \sigma_n)$. Thus $x_{n+1} = x_n + z, y_{n+1} = x_n + z,'$ with $z, z' \in \sigma_n$. But referring to the existence proof, we see $z \equiv e^{-1}\alpha \equiv z'(\operatorname{mod} \sigma_{n+1})$, where $\alpha = 1 - w(1 + x_n)$. Thus $x_{n+1} - y_{n+1} \in \sigma_{n+1}$ and the induction is complete. This completes the proof of 2.1.

REMARK. If n is a unit in A, the theorem applies to $t^n(1+a)^{-1}, a \in \sigma_1$. That is, $(1+a)$ has a unique n$^{\text{th}}$ root in $U_1(A)$. It is given by the usual binomial formula $\sum_{i=0}^{\infty}\binom{1/n}{i}a^i$. In particular $\binom{1/n}{i} \in \mathbf{Z}[1/n]$.

If in addition A is commutative, the content of 2.1 is exactly the ability to extract n$^{\text{th}}$ roots in $U_1(A)$ when n is a unit of A.

COROLLARY 2.3. *If A is a Q–algebra, then $U_1(A)$ is a $\mathcal{D}$–group* [**2**]; *that is, for each $n \neq 0$, the* n$^{\text{th}}$ *power map $x \to x^n$ is a bijection.*

COROLLARY 2.4. *If $w \in U_1(A)\langle t\rangle$ has $e_t(w) = \pm 1$, then $w(t) = 1$ has a unique solution in $U_1(A)$.*

We give two examples of filtered rings. Only the second will be studied in the next section.

EXAMPLE 2.5. Let A be a graded ring. Thus $A = \cup_{i\in\mathbf{N}} A_i, A_i$ an abelian group, and $A_i \cdot A_j \subseteq A_{i+j}$. Let $\sigma_i = \amalg_{j>i} A_j$. Then $A\hat{} = \prod_{i\in\mathbf{N}} A_i$ and $U_1(A\hat{}) = \{(a_i)_{i\in\mathbf{N}}, a_i \in A_i, a_0 = 1\}$.

EXAMPLE 2.6. Let A be a ring and I a two sided ideal. Let $\sigma_n = I^n$. This determines the I–aic filtration on A. In particular, if G is a group and R is commutative ring, we may form $R[G]$, group ring coefficients in R, and let I be the augmentation ideal, kernel of map $R[G] \to R, g \to 1, g \in G$. Then $R[G]$ may be completed in the I–adic topology.

3. Group rings. We want to apply the results of the preceding section to solve equations in groups. We work mainly with the integral group ring $\mathbf{Z}[G]$. Complete in the I–adic topology (I = augmentation ideal) to get $\mathbf{Z}[G]\hat{}$. There is a canonical homomorphism

$$G \xrightarrow{f} U_1(\mathbf{Z}[G]\hat{})$$

given by $f(g) = 1 + (g-1)$; $(g-1) \in I$. To solve equations in G, we need to know when f is injective. The next result gives the answer for fg groups.

THEOREM 3.1. *If f is injective, then G is ω–nilpotent. Conversely, if G is fg and ω–nilpotent, then f is injective.*

PROOF. We know $\mathbf{Z}[G]\hat{}/I^{n}\hat{} = \mathbf{Z}[G]/I^n$ ([**1**; Corollary 10.4]). Let G_n be the kernel of the composition $G \to U_1(\mathbf{Z}[G]\hat{}) \to U_1(\mathbf{Z}[G]/I^n]$. Thus $G_n = \{x \in G | x - 1 \in I^n\}$. We claim G_n/G_{n+1} is a central subgroup of G/G_{n+1}. But if $x \in G, y \in G_n$, then $f(xyx^{-1}) = xyx^{-1} - 1 = (1+(x-1))(y-1)(1+(x^{-1}-1)) \equiv (y-1)(\operatorname{mod} I^{n+1})$ (using $(y-1) \in I^m$). Hence $f(xyx^{-1}) \equiv f(y) \operatorname{mod} I^{n+1}$, or $xyx^{-1}y^{-1} \in G_{n+1}$.

Thus $\{G_n\}$ is a descending central series for G. But $\operatorname{Ker} f = \cap_n G_n$, so if f is injective, $\cap_n G_n = \{1\}$. However, the lower central series $\{\Gamma_n(G)\}$ descends fastest among descending central series, so $\Gamma_n(G) \subseteq G_n$. Thus $\cap_n \Gamma_n(G) = \{1\}$ and G is ω–nilpotent.

Assume now G is fg and nilpotent. By a theorem of K.A. Hirsch, G imbeds in a product $A \times B$ where A is finite nilpotent and B is fg torsion free nilpotent ([**2**, p. 10]) (G is even of finite index in $A \times B$, but we do not need this fact). Consider the commutative diagram.

$$\begin{tikzcd}
G \arrow[r] \arrow[d] & A \times B \arrow[d] & \\
U_1(\mathbf{Z})[G]^\wedge) \arrow[r] & U_1(\mathbf{Z}[A \times B]^\wedge) \arrow[r] & U_1(\mathbf{Z}[A]^\wedge) \times U_1(\mathbf{Z}[B]^\wedge)
\end{tikzcd}$$

If we show $A \to U_1(\mathbf{Z}[A]^\wedge)$ and $B \to U_1(\mathbf{Z}[B]^\wedge)$ are both injective, the result follows for G by a diagram chase.

But for B, fg torsion free nilpotent, Jennings Theorem [**2**, p. 43] asserts that $\cap_n I^n = \{0\}$ where I is the augmentation ideal in $\mathbf{Q}[B]$. Thus $\mathbf{Q}[B] \to \mathbf{Q}[B]^\wedge$ is injective and the result follows by a diagram chase.

As for A, finite nilpotent, $A = \prod_p A_p$ where A_p is the Sylow p–subgroup of A. Another diagram chase shows it suffices to prove $A_p \to U_1(\mathbf{Z}(A_p]^\wedge)$ is injective. But again $\cap_n I^n = \{0\}$, where I is the augmentation ideal of $\mathbf{Z}[A_p]$ [**5**, p. 107, Example 14], and the result follows.

Summarizing, $G \to U_1(\mathbf{Z}[G]^\wedge)$ is injective if G is fg nilpotent. Suppose now G is fg ω–nilpotent. Then the kernel of the canonical map $G \to \prod_n G/\Gamma_n(G)$ is trivial. Consider the commutative diagram

$$\begin{tikzcd}
G \arrow[r, "1-1"] \arrow[d] & \prod G/\Gamma_n(G) \arrow[d, "1-1"'] \\
U_1(\mathbf{Z}[G]^\wedge) \arrow[r] & \prod U_1(\mathbf{Z}[G/\Gamma_n(G)]^\wedge)
\end{tikzcd}$$

The right vertical arrow is injective as the product of injections. The result follows by a diagram chase. This completes the proof of Theorem 3.1.

EXAMPLE 3.2. If $G = \langle t | t^p \rangle, p$ prime, then $\mathbf{Z}[G] = \mathbf{Z}[[x]]/((x+1)^p - 1)$ and $f : G \to U_1(\mathbf{Z}[G]^\wedge)$ is given by $f(t) = x + 1$.

In contrast, $Q[G]^\wedge = Q[[x]]/((x+1)^p - 1) \simeq Q[[x]]/(x) \simeq Q$, since $\frac{(x+1)^p - 1}{x}$ is a unit.

If G is free on $t_1, \cdots, t_n$, then $\mathbf{Z}[G]\hat{} = \mathbf{Z}\{\{x_1, \cdots, x_n\}\}$, completion of the free associative noncommutative algebra on $x_1, \cdots, x_n$. Here $f(t_i) = 1 + x_i$ is the Magnus imbedding [**2**, p. 27].

Let us deduce some corollaries of 3.1.

THEOREM 3.2. *Let G be a fg ω–nilpotent group. Let $w \in G < t >$ have $e_t(w) = \pm 1$. Then $w(t) = 1$ has a unique solution in $U_1(\mathbf{Z}[G]\hat{})$.*

PROOF. We have identified G with its injective image in $U_1(\mathbf{Z}[G]\hat{})$. The result follows from Corollary 2.4.

This result can be viewed as a strengthening of 1.2. In fact, the solution of $w(t) = 1$ is constructed by an algorithmic procedure.

THEOREM 3.3. (MAL'CEV). *If G is a fg torsion free nilpotent group, then G imbeds in a torsion free $\mathcal{D}$–group* [**3**].

PROOF. $G \to U_1(Q[G]\hat{})$ is an imbedding by Jennings theorem. But $U_1(Q[G]\hat{})$ is a $\mathcal{D}$–group by corollary 2.4.

The minimal $\mathcal{D}$–subgroup containing G is called the Mal'cev completion of G and is a functor from fg torsion free groups to $\mathcal{D}$–groups.

REFERENCES

1. Atiyah and Macdonald, *Introduction to Commutative Algebra,* Addison–Wesley, Reading, Massachusetts, 1969.

2. G. Baumslag, *Lecture notes on nilpotent groups,* CBMS publications no. **2** (AMS), 1971.

3. A.I. Mal'cev, *On a class of homogeneous spaces,* AMS translations (1) **9** (1962), 276-307.

4. W.S. Massey, *Algebraic Topology, an introduction,* Harcourt, Brace and Jacanovich, San Diego, CA, 1967.

5. D.S. Passman, *The algebraic structure of group rings,* Wiley Interscience, New York, N.Y., 1977.

6. J.R. Stallings, *Homology and central series of groups,* Jour. of Algebra **2** (1965), 170-181.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF UTAH, SALT LAKE CITY, UT 84112