PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 123, Number 1, January 1995

ON THE INTEGRALITY OF SOME GALOIS REPRESENTATIONS

ROBERT GROSS

(Communicated by William Adams)

ABSTRACT. We find an appropriate topology to put on K, the fraction field of the Iwasawa algebra $\Lambda = \mathbf{Z}_p[[T]]$, so that compact subgroups of $K^\times$ are in fact contained in $\Lambda^\times$. This ensures that Galois representations to $K^\times$ have image in $\Lambda^\times$.

Let $\Lambda = \mathbf{Z}_p[[T]]$ be the Iwasawa algebra. Λ is a unique factorization domain. The p-adic Weierstrass Preparation Theorem says that elements of Λ may be represented as uf, where f is a polynomial and u is a unit.

Let $M = (p, T)$ be the maximal ideal of Λ. Topologize Λ so that a base of neighborhoods of 0 is given by powers of M, and define neighborhoods of other elements of Λ by translation.

Let K be the field of fractions of Λ. The first question to consider is how to topologize K. One somewhat obvious approach is to say that a set $U \subseteq K$ is open in K precisely when $kU \cap \Lambda$ is an open subset of Λ for all $k \in K^\times$. This definition makes addition and multiplication continuous. Topologized in this way, a compact subset of $\mathrm{GL}_n(K)$ which is also a subgroup is conjugate to a subset of $\mathrm{GL}_n(\Lambda)$. Unfortunately, there is one major drawback to this topology.

Proposition. *The function $f(x) = x^{-1}$ is not continuous in this topology.*

Proof. There are many ways to see this. Perhaps the simplest is to observe that the sequence $a_n = p + T^n$ converges to p. However, the sequence a_n^{-1} is closed, since for a fixed $k \in K^\times$, ka_n^{-1} will be an element of Λ for only finitely many n. Hence, a_n^{-1} cannot converge to p^{-1}.

We therefore need a different topology on K, and fortunately there is an obvious candidate. If $\lambda \in \Lambda$, we can define $v(\lambda) = n$ if $\lambda \in M^n$ and $\lambda \notin M^{n+1}$ and $v(0) = \infty$. Krull's Theorem [1] implies that $\bigcap M^n = \{0\}$, and so the function v is well defined.

Lemma. *v is a valuation on Λ.*

Proof. Let $f, g \in \Lambda$. Set $v(f) = m$ and $v(g) = n$. Obviously, $v(f+g) \geq \min(v(f), v(g))$, so we need only show that $v(fg) = v(f) + v(g)$.

Received by the editors August 19, 1992 and, in revised form, April 14, 1993.
1991 *Mathematics Subject Classification.* Primary 22C05, 11S20.
Key words and phrases. Compact groups, Iwasawa algebra.

Use the Weierstrass Preparation Theorem to write $f = u_1 f'$, $g = u_2 g'$, where u_1 and u_2 are units and f' and g' are polynomials. Write $f' = \sum a_i T^i$ and $g' = \sum b_j T^j$. Let v_p be the usual p-adic valuation on $\mathbf{Z}_p$. Of those terms in $\sum a_i T^i$ with $v(a_i T^i) = m$, let $a_k T^k$ be the term so that $v_p(a_k)$ is minimal. (It is easy to see that there is a unique minimum, because if $v(a_i T^i) = m$, then $v_p(a_i) = m - i$.) Similarly, let $b_l T^l$ be the term in the second sum minimizing $v_p(b_l)$ subject to $v(b_l T^l) = n$.

If we now consider the coefficient c_{k+l} of T^{k+l} in the product $fg = u_1 u_2 f' g'$, we see that $v_p(c_{k+l}) = v_p(a_k) + v_p(b_l)$. Therefore, $v(c_{k+l} T^{k+l}) = m + n$, and we finally have $v(fg) = m + n$.

This lemma in fact is true in considerably greater generality, but the statement does not seem to appear in the literature in this form.

Because Λ is a unique factorization domain, we can extend v to K by defining $v(f/g) = v(f) - v(g)$, and the valuation still is well defined. Let

$$R = \{k \in K : v(k) \geq 0\}$$

and

$$P = \{k \in K : v(k) > 0\}.$$

Notice that R is a discrete valuation ring and P is the unique maximal ideal. In fact, P is principal, and we choose p as a generator.

Proposition. $R/P \cong \mathbf{F}_p(t)$.

Proof. Though this fact appears to be well known to valuation theorists, there is no statement of it in the number-theoretic literature, so we sketch a proof.

Let $k \in K$ be an element with $v(k) = 0$. We can write $k = \frac{f}{g}u$, where $u \in \Lambda^\times$ and $f, g \in \mathbf{Z}_p[T]$. Let $v(f) = v(g) = n$. Then f/p^n and g/p^n are elements of $\mathbf{Z}_p[\frac{T}{p}]$. The reduction modulo P now sends $\frac{T}{p}$ to t, u to its constant term, and $\mathbf{Z}_p$ to $\mathbf{F}_p$.

Corollary. *R is neither compact nor locally compact.*

Proof. Because R/P is infinite, we can cover R with an infinite cover of the form $a + P$ with no finite subcover. Similarly, any neighborhood of 0 contains P^k for some k, and P^k/P^{k+1} is an infinite group.

If we now consider a continuous Galois representation ρ with image in K, a priori, such a representation must have image in $R^\times$ because the image must be compact. However, the preceding proposition gives us reason to hope that we can do considerably better.

Proposition. *Compact subgroups of $K^\times$ are subgroups of $\Lambda^\times$.*

Proof. Let G be a compact subgroup of $K^\times$. Let $a \in G$. The closure of the set $\{a^n : n \in \mathbf{Z}\}$ must be compact, which means that $v(a) = 0$. If we now reduce $\{a^n\}$ modulo P, we get an image that is a compact subgroup of $\mathbf{F}_p(t)$. Since $\mathbf{F}_p(t)$ has the discrete topology, the reduction of $\{a^n\}$ must be a finite subgroup. Hence, the reduction maps not just to $\mathbf{F}_p(t)$, but to $\mathbf{F}_p$. Let $b = a^{p-1}$, and then $b \equiv 1 \pmod{P}$.

Because P is principal, we can write $b = 1 + pr$, where $r \in R$. Using the fact that $v_p(\binom{p^k}{m}) = k - v_p(m)$ for $1 \leq m \leq p^k$, it is simple to show that

$$(*) \qquad \lim_{n\to\infty} b^{p^n} = 1.$$

Let c be any element of $\mathbf{Z}_p$, and write $c = \lim c_n$, where $c_n \in \mathbf{Z}$. The set $\{b^{c_n}\}$ is contained in G, and hence must have a convergent subsequence; however, since $c = \lim c_n$, $(*)$ means that all subsequences must converge to the same limit, which we might as well denote by b^c.

In particular, we may let $c = (1+p^i)^{-1}$, for any positive integer i. The preceding discussion shows that $b^{1/(1+p^i)}$ is an element of K for any positive integer i. Write $b = \frac{f}{g}u$, where f and g are relatively prime, and then we may conclude that $(1+p^i)|v(g)$ for all positive integers i. That, in turn, forces $v(g) = 0$, and then b must be an element of Λ. Since this argument applies to f as well, b is a unit in Λ. Because Λ is integrally closed in K, we see that $a \in \Lambda^\times$ as well.

Notice that a key feature of this argument is that K is not complete, though Λ is.

Corollary. *Suppose that* $\rho : \mathrm{Gal}(\overline{\mathbf{Q}_p}/\mathbf{Q}_p) \to K^\times$ *is a continuous Galois representation. Then the image of* ρ *is contained in* $\Lambda^\times$.

Though the above result is already of considerable interest in Hida theory, representations to $\mathrm{GL}_2(K)$ are of much more interest. It is tempting to

Conjecture. *Suppose that* $\rho : \mathrm{Gal}(\overline{\mathbf{Q}_p}/\mathbf{Q}_p) \to \mathrm{GL}_n(K)$ *is a continuous Galois representation. Then the image of* ρ *is conjugate to a subgroup of* $\mathrm{GL}_n(\Lambda)$.

Unfortunately, the above methods do not suffice to prove this conjecture. A generalization, using a localization argument, proves only that eigenvalues of a matrix in the image of ρ are units in the integral closure of Λ in an extension of K.

Acknowledgment

Thanks to Ralph Greenberg for posing this question, and to both Glenn Stevens and Ralph Greenberg for many helpful conversations.

References

1. Nicolas Bourbaki, *Commutative algebra*, Springer Verlag, New York, 1989, p. 200.

Department of Mathematics, Boston College, Chestnut Hill, Massachusetts 02167-3806

E-mail address: gross@bcvms.bc.edu