



---

Automorphisms of  $p$ -Adic Number Fields

Author(s): C. G. Wagner

Source: *The American Mathematical Monthly*, Vol. 81, No. 1 (Jan., 1974), pp. 51-52

Published by: Mathematical Association of America

Stable URL: <http://www.jstor.org/stable/2318914>

Accessed: 28/04/2010 14:09

---

Your use of the JSTOR archive indicates your acceptance of JSTOR's Terms and Conditions of Use, available at <http://www.jstor.org/page/info/about/policies/terms.jsp>. JSTOR's Terms and Conditions of Use provides, in part, that unless you have obtained prior permission, you may not download an entire issue of a journal or multiple copies of articles, and you may use content in the JSTOR archive only for your personal, non-commercial use.

Please contact the publisher regarding any further use of this work. Publisher contact information may be obtained at <http://www.jstor.org/action/showPublisher?publisherCode=maa>.

Each copy of any part of a JSTOR transmission must contain the same copyright notice that appears on the screen or printed page of such transmission.

JSTOR is a not-for-profit service that helps scholars, researchers, and students discover, use, and build upon a wide range of content in a trusted digital archive. We use information technology and tools to increase productivity and facilitate new forms of scholarship. For more information about JSTOR, please contact [support@jstor.org](mailto:support@jstor.org).



Mathematical Association of America is collaborating with JSTOR to digitize, preserve and extend access to *The American Mathematical Monthly*.

<http://www.jstor.org>

Finally we note that a group can satisfy both chain conditions on normal subgroups and have infinitely many normal subgroups.

**THEOREM 4.** *A group  $G$  satisfying both chain conditions on normal subgroups has infinitely many normal subgroups if and only if there is a normal subgroup  $N$  of  $G$ , a group  $H$  and a simple  $H$ -module  $A$  with  $\text{Aut}_H(A)$  infinite such that  $G/N$  is an extension of  $A \times A$  by  $H$  inducing the given operation of  $H$  on  $A$ .*

An example of such a group is provided by the semidirect product of  $R^3 \oplus R^3$  by  $SO_3$  where  $R^3$  is Euclidean 3-space and  $SO_3$  is its group of rotations.

A. W. HALES: DEPARTMENT OF MATHEMATICS, UNIVERSITY OF CALIFORNIA, LOS ANGELES, CALIFORNIA 90024.

R. J. NUNKE: DEPARTMENT OF MATHEMATICS, UNIVERSITY OF WASHINGTON, SEATTLE, WASHINGTON 98109.

### AUTOMORPHISMS OF $p$ -ADIC NUMBER FIELDS

C. G. WAGNER

In 1933 F. K. Schmidt [4, p. 3] proved a theorem which characterizes those fields which are complete with respect to at least two non-trivial inequivalent absolute values. A corollary of Schmidt's theorem states that a field complete with respect to a discrete absolute value is not complete with respect to an absolute value inequivalent to the original. An application of this corollary is the following standard proof of the fact that the identity map is the only automorphism of the field  $Q_p$  of  $p$ -adic numbers: Let  $g$  be an automorphism of  $Q_p$  with  $p$ -adic absolute value  $|\cdot|_p$ , and define an absolute value  $|\cdot|_g$  on  $Q_p$  by  $|\alpha|_g = |g^{-1}(\alpha)|_p$  for all  $\alpha \in Q_p$ . Then  $Q_p$  is complete with respect to  $|\cdot|_g$ ,  $|\cdot|_p$  and  $|\cdot|_g$  agree on  $Q$ , and  $|\alpha|_p = |g(\alpha)|_g$  for all  $\alpha \in Q_p$ . Since  $|\cdot|_p$  and  $|\cdot|_g$  are equivalent, they agree on  $Q_p$ , and so  $|\alpha|_p = |g(\alpha)|_p$  for all  $\alpha \in Q_p$ . Hence  $g$  is continuous and is, thus, the identity map.

It may be of interest to note that there is an alternative "elementary" proof that any automorphism of  $Q_p$  is continuous, based on the fact that such an automorphism must preserve the units of  $Q_p$ . That this is the case is an obvious consequence of the following algebraic characterization of the units.

**THEOREM.** *Let  $\alpha \in Q_p$ . Then  $|\alpha|_p = 1$  if and only if  $\alpha$  has an  $m$ -th root in  $Q_p$  for all positive integers  $m$  prime to  $p(p-1)$ .*

*Proof. Sufficiency.* Immediate from the fact that the range of  $|\cdot|_p$  is the discrete set  $\{0, p^n: n \in Z\}$ .

*Necessity.* Since  $|\alpha|_p = 1$ ,  $\alpha = a_0 + a_1p + a_2p^2 + \dots$ , where  $0 \leq a_i < p$  and  $a_0 \neq 0$ . Consider the polynomial  $f(x) = x^m - \alpha$ . Since  $(m, p-1) = 1$ , it follows

from a well-known fact about power congruences [3, p. 95] that there exists a natural number  $a$  such that  $0 < a < p$  and  $a^m \equiv a_0 \pmod{p}$ . Hence  $|f(a)|_p < 1$  and, since  $(m, p) = 1$  and  $0 < a < p$ ,  $|f'(a)|_p = |ma^{m-1}|_p = 1$ . Thus by Newton's method [2, p. 52] we may construct a sequence in  $\mathcal{Q}_p$  which converges to a root of  $f(x)$ .

We remark that Ax and Kochen have proved a more general version of the preceding theorem as part of their study of formally  $p$ -adic fields [1, p. 633].

I wish to thank the referee for calling Schmidt's paper to my attention.

#### References

1. J. Ax and S. Kochen, Diophantine problems over local fields, II, Amer. J. Math., 87 (1965) 631-648.
2. G. Bachman, Introduction to  $p$ -adic Numbers and Valuation Theory, Academic Press, New York, 1964.
3. C. Long, Elementary Introduction to Number Theory, Heath, Boston, 1965.
4. F. K. Schmidt, Mehrfach perfekte Körper, Math. Ann., 108 (1933) 1-25.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF TENNESSEE, KNOXVILLE, TENNESSEE 37916.

### A POINCARÉ TYPE COINCIDENCE THEOREM

SIMEON REICH

Let  $B$  denote the unit ball of a finite-dimensional Euclidean space  $E$ . According to Brouwer's fixed point theorem a continuous  $g: B \rightarrow B$  has a fixed point. Let  $S$  denote the boundary of  $B$ . Recall that two functions  $f$  and  $g$  which map a set  $X$  into another set  $Y$  are said to have a coincidence if there exists a point  $x \in X$  such that  $f(x) = g(x)$ . Schirmer [3] has established the following interesting coincidence theorem:

**THEOREM 1.** *Let  $f$  and  $g$  map  $B$  continuously into itself, and suppose that  $f(S) \subset S$ . If  $f|_S: S \rightarrow S$  is not nullhomotopic, then  $f$  and  $g$  have a coincidence.*

This proposition formally includes Brouwer's theorem because the identity map on  $S$  is not nullhomotopic. Of course, Brouwer's theorem is an immediate consequence of this (highly non-trivial) fact [1, p. 341].

Schirmer's proof is somewhat complicated. In this note we present a very simple proof of an extension of Theorem 1. It seems to be difficult to obtain this extension by adapting Schirmer's arguments. In the sequel, if  $0 \neq x \in E$ , then the point  $x/|x|$ , which belongs to  $S$ , will be denoted by  $p(x)$ .

**THEOREM 2.** *Let  $f$  and  $g$  map  $B$  continuously into  $E$ , and suppose that  $f(S) \subset S$ . If  $f|_S: S \rightarrow S$  is not nullhomotopic and  $g(y) \neq mf(y)$  for all  $y \in S$  and  $m > 1$ , then  $f$  and  $g$  have a coincidence.*