PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 28, No. 1, April 1971

A WEAK NULLSTELLENSATZ FOR VALUATIONS

GEORGE M. BERGMAN[1]

ABSTRACT. Given a real-valued pseudovaluation p on a commutative ring R, we show how to obtain a valuation v greater than or equal to p, and also satisfying certain upper bounds: in particular, if $p(st)=p(s)+p(t)$ for all $s, t\in S$, S a multiplicative semigroup in R, then v can be chosen so that $v(s)=p(s)$ for all $s\in S$.

1. An important lemma of commutative ring theory—a form of the "weak Nullstellensatz"—says that given an ideal I of a ring R, and a multiplicative semigroup S in R disjoint from I, there exists a prime ideal $\mathfrak{p}$ containing I, and still disjoint from S.

Now a pseudovaluation on a ring can be considered analogous to an ideal—an ideal tells us which elements to "consider 0", a pseudovaluation tells us which elements to "consider small". In particular, the *valuations* are like the prime ideals. We shall prove here some analogs to the lemma quoted above, showing how to obtain valuations from pseudovaluations.

The desire to give the strongest possible result has made the statement of our first theorem (and the two lemmas used to prove it) rather complicated. But the special cases that follow it are more modest, and more handleable.

The analogy with ideal theory can be made precise by noting that there is a 1-1 correspondence between ideals in R, and pseudovaluations of R into the two-element additive semigroup $\{0, +\infty\}$. Each of the results proved below, if stated for this semigroup rather than $\mathbf{R}\cup\{+\infty\}$, is a result about ideals; and these statements follow from those proved via the observation that $\{0, +\infty\}$ is a *retract* of $\mathbf{R}\cup\{+\infty\}$, as ordered semigroups.

2. Let R be a commutative associative ring with unit. We will designate by $\mathbf{P}$ the additive ordered semigroup of real numbers with $+\infty$ adjoined.

DEFINITIONS. *By a* pseudovaluation *on R, we shall mean a function $p: R\to\mathbf{P}$ satisfying*:

$$p(1) = 0, \qquad p(0) = +\infty, \tag{1}$$

Received by the editors February 10, 1970.
AMS 1970 *subject classifications*. Primary 13A15; Secondary 12J20, 14A05.
Key words and phrases. Valuation, pseudovaluation, Nullstellensatz.

[1] Work done while the author held a research fellowship from the Science Research Council (England).

$$p(xy) \geqq p(x) + p(y) \qquad (x, y \in R), \tag{2}$$

$$p(x - y) \geqq \inf(p(x), p(y)) \qquad (x, y \in R). \tag{3}$$

The pseudovaluation p will be called radical *if it satisfies*:

$$p(x^n) = np(x) \qquad (x \in R, n > 0). \tag{4}$$

By a valuation *we shall mean a pseudovaluation satisfying the stronger condition*:[2]

$$p(xy) = p(x) + p(y) \qquad (x, y \in R). \tag{5}$$

Radical pseudovaluations will play the role of radical (or "perfect") ideals.

In the statements below, a supremum of the form $\sup_{s \in S} p(xs) - p(s)$ will be understood to be taken only over the set of $s \in S$ such that $p(s) \neq +\infty$. This set will always be nonempty because every semigroup S will be understood to contain 1.

Our first lemma describes the operation of "radicalizing" a pseudovaluation. The idea is not new, cf. [1, Theorem 9.4]. The significance of the final inequality is that certain types of upper bounds for $p(x)$ are not increased; this will allow us to obtain upper as well as lower bounds for the valuations to be constructed in Theorem 1 and later results.

LEMMA 1. *Let p be a pseudovaluation on R. Then the function $p^*(x) = \lim_{n \to \infty} p(x^n)/n$ is defined for all $x \in R$, and is a radical pseudovaluation, $\geqq p$. Further, if x is an element of R, and S a multiplicative semigroup containing x, then*

$$\sup_{s \in S} p^*(xs) - p^*(s) \leqq \sup_{s \in S} p(xs) - p(s).$$

PROOF. Take $x \in R$; we wish to prove $p^*(x)$ defined and $\geqq p(x)$. If some $p(x^n)$ equals $+\infty$, this is clear. Assuming all $p(x^n)$ finite, we have for every positive integer N:

$$\liminf p(x^n)/n = \inf_{i=0,\ldots,N-1} \left(\liminf_m p(x^{mN+i})/(mN + i) \right)$$

$$\geqq \inf_{i=0,\ldots,N-1} \left(\liminf_m p(x^{mN})/(mN + i) + \liminf_m p(x^i)/(mN + i) \right).$$

The second term is clearly 0. The first gives, regardless of i:

[2] The term (pseudo)valuation is often used with the additional restriction that the ideal $I = p^{-1}(+\infty) \subseteq R$ be $\{0\}$. In such terms, the functions we are considering are equivalent to (pseudo)valuations on quotient rings R/I, or in the language of the algebraic geometer, (pseudo)valuations "centered" on subschemes of Spec R.

$$\liminf_m p(x^{mN})/mN \geqq p(x^N)/N \qquad \text{(by condition (2))}.$$

Comparing with what we started from, we see that the lim inf in question will also be the supremum of its terms, hence will be their limit.

That conditions (1) and (2) carry over to p^* is immediate, and (4) follows from the way p^* was constructed. To prove (3), let us expand $(x+y)^n$ using repetitions of terms instead of binomial coefficients. Applying condition (3), we see:

$$\begin{aligned} p^*(x+y) &= \lim_n p((x+y)^n)/n \\ &\geqq \lim_n \min_{i \leqq n} (p(x^i) + p(y^{n-i}))/n \\ &= \lim_n \min_{i \leqq n} \left(\frac{i}{n} \frac{p(x^i)}{i} + \frac{n-i}{n} \frac{p(y^{n-i})}{n-i} \right). \end{aligned}$$

We now note that when i and $n-i$ are both large, $p(x^i)/i$ will be near $p^*(x)$ and $p(y^{n-i})/(n-i)$ will be near $p^*(y)$, and the sum in the above formula is a convex linear combination of these. If n is large and i/n is small, the sum will be near to $p^*(y)$ (unless $p^*(x) = +\infty$, in which case it may be larger), and similarly, if n is large and $(n-i)/n$ small, it will be near to or larger than $p^*(x)$. We conclude that for n large, the minimum in the above formula will be near to or larger than $\min(p^*(x), p^*(y))$, so the limit is $\geqq \min(p^*(x), p^*(y))$. Q.E.D.

To obtain the last inequality asserted, let us denote the supremum on the right by $q(x)$; thus taking any particular $t \in S$, we have $p(tx) \leqq p(t) + q(x)$. Since $x \in S$, we can, for any $s \in S$, and $n > 0$, apply this property recursively to $x^n s^n$:

$$p(x^n s^n) \leqq p(x^{n-1} s^n) + q(x) \leqq \cdots \leqq p(s^n) + nq(x).$$

Dividing by n and taking the limit, we get $p^*(xs) \leqq p^*(s) + q(x)$; hence if $p^*(s) \neq +\infty$, $p^*(xs) - p^*(s) \leqq q(x)$, as desired. ∎

Let us say that an element x is *regular* under p, or p is regular on x, if for all y, $p(xy) = p(x) + p(y)$.

LEMMA 2. *Let p be a radical pseudovaluation on R, and x an element with $p(x) \neq +\infty$. Then the function $p_x(y) = \lim_{n\to\infty} p(yx^n) - np(x)$ is defined for all $y \in R$, and is a radical pseudovaluation $\geqq p$, which is regular on x. Further, for any $y \in R$ and any multiplicative semigroup S containing x, we have:*

$$\sup_{s \in S} p_x(ys) - p_x(s) \leqq \sup_{s \in S} p(ys) - p(s).$$

PROOF. The sequence $p(yx^n)-np(x)$ converges because it is non-decreasing, by (2). The verifications of conditions (1), (3), (4) for p_x are straightforward. For (2), let $u, v \in R$; then $p_x(uv)$, $p_x(u)$ and $p_x(v)$ can be arbitrarily closely approximated by $p(uvx^{2n})-2np(x)$, $p(ux^n)-np(x)$, and $p(vx^n)-np(x)$ for sufficiently large n. By (2) for p, we see that $p(uvx^{2n})-2np(x) \geqq (p(ux^n)-np(x))+(p(vx^n)-np(x))$, whence $p_x(uv) \geqq p_x(u)+p_x(v)$.

We get the asserted inequality similarly: Each term $p_x(ys)-p_x(s)$ may be approximated by expressions $(p(ysx^n)-np(x))-(p(sx^n)-np(x))=p(y(sx^n))-p(sx^n)$; but each of these is a term of the right-hand supremum (because $x \in S$). ■

Note that if an element y is regular under p, then the special inequality proved in Lemma 1 (resp. Lemma 2), with S taken to be R, implies that y remains regular under p^*(resp. p_x), and $p^*(y)=p(y)$ (resp. $p_x(y)=p(y)$).

If $p(x)=+\infty$, we define p_x to be p. This has all the properties proved in Lemma 2.

THEOREM 1. *Let p be a pseudovaluation on a commutative ring R. Then there exists a valuation v on R satisfying*:

$$p(x) \leqq v(x) \leqq \sup_{s \in R} p(xs) - p(s) \qquad (x \in R). \tag{6}$$

In fact, if we are given any set-theoretic total ordering of R, then v can be chosen so that (6) *is satisfied with the supremum on the right taken over only the semigroup S_x generated by elements $\leqq x$ under this ordering.*

PROOF. Let us think of pseudovaluations $\geqq p$ as certain points in the compact product of intervals $\Pi_{x \in R}\,[p(x), +\infty]$.

Assume R totally ordered. To every finite chain $x_1 < x_2 < \cdots < x_n$ in R, let us associate the pseudovaluation $(\cdots (p^*)_{x_1} \cdots)_{x_n}$, which is radical, and is regular on $x_1, \cdots, x_n$. Considering our index set of finite subsets of R as directed by inclusion, we have a net of points in a compact space; let v be a cluster point of this net.

It is immediate that v will be a pseudovaluation, and regular on all elements, hence a valuation. To prove that for every $x \in R$ we have:

$$p(x) \leqq v(x) \leqq \sup_{s \in S_x} p(xs) - p(s), \tag{6'}$$

we shall show that the same inequality holds for the pseudovaluation associated with any chain $x_1 < \cdots < x_n$ containing x. Say $x = x_i$. For $j=1, \cdots, n$, let p_j stand for $(\cdots (p^*)_{x_1} \cdots)_{x_j}$. Let $q(x)$ designate $\sup_{s \in S_x} p(xs)-p(s)$, and let $q^*, q_1, \cdots, q_n$ be constructed in the same way from $p^*, p_1, \cdots, p_n$. Noting that S_x is a semigroup containing

$x_1, \cdots, x_i$, we can conclude from Lemmas 1 and 2 that:

$$p(x) \leqq p^*(x) \leqq p_1(x) \leqq \cdots \leqq p_i(x) = q_i(x) \leqq \cdots \leqq q^*(x) \leqq q(x).$$

The central equality holds because p_i is regular on x. But by the observation following Lemma 2, this equality means that the value at x is not affected by further regularizations, hence $p_n(x) = p_i(x)$, and, $p(x) \leqq p_n(x) \leqq q(x)$. Q.E.D.

(The above compactness argument may be replaced by a more familiar Zorn's Lemma argument if R is not ordered, using the fact that the set of radical pseudovaluations satisfying (6) is inductively ordered under "$\geqq$", and closed under regularizations; or by an induction if R is *well*-ordered.) ∎

Let us chop this down to something more manageable:

THEOREM 2. *Let p be a pseudovaluation on a commutative ring R, and S a multiplicative semigroup in R such that $p \mid S$ is a semigroup homomorphism from S to* **P**. *Then there exists a valuation $v \geqq p$ on R, such that $v \mid S = p \mid S$.*

PROOF. Choose a partial ordering of R such that all elements of S precede all elements not in S. Apply Theorem 1, noting that for $x \in S$, the first and last terms of (6′) are equal, implying $v(x) = p(x)$. ∎

The next statement mixes valuations and ideals, but avoids mention of pseudovaluations. Note that the hypothesis on S and I is a sort of strong disjointness relative to v:

COROLLARY 1. *Let R be a ring and v a valuation on R. Let I be an ideal of R and S a multiplicative semigroup such that there do not exist $s \in S$, $a \in I$ satisfying $v(s) = v(a) < v(a-s)$. Then there exists a valuation $v' \geqq v$ on R such that $v' \mid I = +\infty$, $v' \mid S = v \mid S$.*

PROOF. The function $p(x) = \sup_{a \in I} v(x+a)$ will be a pseudovaluation on R, and our hypothesis implies that $p = v$ on S. In particular, $p \mid S$ is a semigroup homomorphism, hence we can apply Theorem 2 and get the desired v'. ∎

We now give an analog of a familiar characterization of radical ideals. (This result was proved by Cohn for R a field [1, Theorem 13.3].)

COROLLARY 2. *A psuedovaluation on a ring R is equal to an infimum of valuations if and only if it is radical. If p is an arbitrary pseudovaluation, the infimum of all valuations $\geqq p$ is p^*.*

PROOF. It is clear that the pointwise infimum of a family of valuations (if it is defined!) is a radical pseudovaluation. Thus it suffices to show that if p is a radical pseudovaluation, then for each $x \in R$ there

is a valuation $v \geqq p$ such that $v(x) = p(x)$. This follows from Theorem 2 on taking $S = \{1, x, x^2, \cdots\}$. The second claim follows because it is clear that p^* is the least radical pseudovaluation $\geqq p$. ∎

NOTE. If a pseudovaluation p on a ring R annihilates a multiplicative sub*group* $G \subseteq R$, then so will any pseudovaluation $p' \geqq p$, by (1) and (2). In particular in the above results, if R is an algebra over a field k and the given pseudovaluations annihilate $k - \{0\}$, so will the valuations constructed.

3. We shall now sketch two examples to show that the above constructions cannot in general be made to carry the class of pseudovaluations satisfying $p^{-1}(+\infty) = \{0\}$ into itself.

First, let R be a polynomial ring in one indeterminate x over a field k, and define the valuation v by $v(a) =$ greatest i such that x^i divides a. Then $p(a) = v(a)^2$ defines a pseudovaluation, but $p^*(x) = +\infty$, so no valuation $\geqq p$ satisfies $v'^{-1}(+\infty) = \{0\}$.

Now let R be the polynomial ring in two indeterminates x and y over a field k of characteristic 0. For each $n = 1, 2, \cdots$, the members of R restricted to the line $x = n$ give polynomials in y alone. Let $v_n(a)$ denote the greatest i such that y^i divides the restriction of a to $x = n$. This will be a valuation satisfying $v_n^{-1}(+\infty) = (x-n)R$.

Define $p = \inf_n nv_n$; p is a radical pseudovaluation, and $p^{-1}(+\infty) = \{0\}$. Note that $p(y^n(x-1)\cdots(x-n)) = n(n+1)$, and p is zero on $k - \{0\}$. The latter property will be shared by any (pseudo) valuation $\geqq p$.

But now let us observe that if v is any pseudovaluation on R equal to zero on nonzero members of the base field, then, since any three of the elements $x - i$ are linearly dependent over this base field, $v(x-i)$ can assume no more than two distinct values for $i = 1, \cdots$. In particular, if this v is a valuation, and is $< +\infty$ at y and at all $x - i$, we can obtain a bound of the form $v(y^n(x-1)\cdots(x-n)) \leqq cn$. But p does not satisfy such a bound, so any valuation $\geqq p$ must assume the value $+\infty$ on y or some $x - i$.

Note, however, that if p is any pseudovaluation on a *field*, the ideal $p^{-1}(+\infty)$ is necessarily zero.

4. **Generalizations.** If p is a valuation on a ring R, and α a real number, $0 < \alpha < 1$, then the function $m(x) = \alpha^{p(x)}$ is an ultrametric multiplicative pseudovaluation on R, that is, a nonnegative real-valued function satisfying:

$$(1') \qquad m(1) = 1, \quad m(0) = 0,$$

$$(2') \qquad m(xy) \leqq m(x)m(y),$$

$$(3') \qquad m(x - y) \leqq \sup(m(x), m(y)).$$

Our above results all translate directly into facts about such multiplicative valuations and pseudovaluations. It is natural to ask whether the same results hold for the related classes of functions in which the ultrametric inequality (3′) is replaced by the weaker triangle inequality:

$$(3'') \qquad m(x - y) \leqq m(x) + m(y).$$

In fact, they do. The only proof that we cannot adapt essentially verbatim from §2 (interchanging 0 and $+\infty$, etc.) is of the fact that radicalization preserves the triangle inequality. The radical of m is defined by $m^*(x) = \lim_n m(x^n)^{1/n}$. We find that

$$m((x-y)^n) \leqq \sum \binom{n}{i} m(x^i)\, m(y^{n-i}).$$

For any $\epsilon > 0$, we can show that for n sufficiently large, each of the terms $m(x^i)m(y^{n-i})$ approximates $m^*(x)^i m^*(y)^{n-i}$ to within a factor of $(1+\epsilon)^n$, hence the sum approximates $(m^*(x)+m^*(y))^n$ to within such a factor, hence, taking nth roots and letting n approach infinity, $m^*(x-y) \leqq m^*(x)+m^*(y)$.

Returning to additive valuations as in preceding sections, we would like to know whether the results we have proved can be generalized to valuations into semigroups of the form $A \cup \{+\infty\}$, for arbitrary ordered abelian groups A. The real numbers and $\{0\}$ are the only ordered groups in which we can both divide by integers (for radicalizing) and take limits of bounded ascending sequences. For any other A, we must expect in general that the valuation v we construct from an A-valued pseudovaluation p will not be into A itself, but some extension of A. The formal statements of our results would also have to be modified: for instance, inequalities between suprema of infinite sets would have to be changed to statements that every upper bound for one set is an upper bound of the other, because the suprema themselves might not exist.

But we have not succeeded in proving any such generalizations of our results.

Note that if we look for A in which we can take least upper bounds of bounded sets, but not necessarily divide by integers, there are not only $\{0\}$ and $\mathbf{R}$, but also $\mathbf{Z}$. Hence one can prove that if p in the hypothesis of Theorem 1 is already radical, and is $\mathbf{Z} \cup \{+\infty\}$-valued, the v of the conclusion can also be taken $\mathbf{Z} \cup \{+\infty\}$-valued.

Reference

1. P. M. Cohn, *An invariant characterization of pseudo-valuations on a field*, Proc. Cambridge Philos. Soc. **50** (1954), 159–177. MR **16**, 214.

Bedford College, London N.W.1, England

University of California, Berkeley, California 94720