JOURNAL OF
PURE AND
APPLIED ALGEBRA

ELSEVIER Journal of Pure and Applied Algebra 111 (1996) 277–284

Discrete rings

Niel Shell

The City College of New York (CUNY), Convent Avenue at 138th Street, New York, NY 10031, USA

Communicated by M.-F. Roy; received 20 November 1994; revised 14 March 1995

Abstract

Discretely topologized subrings of fields with an absolute value are considered.

We use $\mathbf{Z}$, $\mathbf{Q}$, $\mathbf{R}$, $\mathbf{C}$, and $E_{>0}$ to denote the set of all rational integers, rational numbers, real numbers, complex numbers and positive elements of a subset E of $\mathbf{R}$, respectively. The symbols $|\ |_\infty$ and $\mathcal{T}_\infty$ will denote the usual absolute value and the usual topology on any subfield of $\mathbf{C}$.

If E is a subset of an algebraic structure containing 0, then E^* denotes $E\backslash\{0\}$. In a ring R with identity e, we usually denote by n and $\mathbf{Z}$ (rather than $n \cdot e$ and $\mathbf{Z} \cdot e$) the integer n in R and the ring of integers of R. We say a ring has *pure characteristic* n (*pure characteristic* 0) if the order of each nonzero element of the additive group of the ring is n (respectively, infinity). By a ring of pure characteristic we mean a ring of pure characteristic n for some $n \geq 0$. Obviously, each field is a ring of pure characteristic. Recall that an *order* of a field F is a subring of F containing the identity and having quotient F.

Also recall that a field with an absolute value is either a rank one nonarchimedean valued field or a subfield of the complex numbers with a power of the usual absolute value (see, e.g., [4, Theorems 12.1.1 and 15.2.2]).

Containment is the partial order for a collection of ring topologies considered as a lattice. The notation $\vee E$ or $a \vee b$ denotes a supremum, and $\wedge E$ or $a \wedge b$ denotes an infimum. The trivial and discrete topologies on any set will be denoted by $\mathbf{0}$ and $\mathbf{1}$, respectively.

If U is a bounded neighborhood of zero in some ring topology on a field F, U determines this topology uniquely, since $\{aU : \ a \in F^*\}$ is a neighborhood base at zero; $\mathcal{T}_U$ will denote this topology.

By a *discrete* subring (subgroup) of a topological ring (group) we mean a subring (subgroup) which is discretely topologized in the induced topology.

SSDI 0022-4049(95)00107-7

In [2], the fact that $\mathbf{Z}$ is discrete in $(\mathbf{Q}, \mathcal{T}_\infty)$ was used to define ring topologies on $\mathbf{Q}$ finer than $\mathcal{T}_{\mathbf{Z}}$. In [4] it was observed that the same construction could be used to define ring topologies on any field with an absolute value that contained a discrete subring whose quotient is the field. In [5, 6], it was observed that a similar technique generalized two constructions of Mutylin of ring topologies on $\mathbf{Q}$ that are not finer than any topology induced by a valuation. (The best known open question in the theory of commutative topological fields is whether or not there is a minimal ring topology which is not induced by a valuation; and examples of ring topologies not finer than any topology induced by a valuation may help answer this question.) We consider here the problem of finding discrete subrings of fields with an absolute value.

This is a special case of the following fairly natural problem: Describe all discrete subrings (subgroups) of a topological ring (topological group).

By homogeneity, it is obvious that a subgroup H of a topological group G with identity e is discrete if and only if $H \setminus \{e\}$ is bounded away from e. A discrete subgroup of a Hausdorff topological group must be closed: If the subgroup H clusters at any point $a \in G$, then $H = H^{-1}$ clusters at a^{-1}. If U is a neighborhood of the identity in G, then there are $h, k \in H$ such that $h \in Ua$ and $k \in a^{-1}U \setminus \{h^{-1}\}$, so $hk = (ha^{-1})(ak) \in (UU) \setminus \{e\}$. Thus, H clusters at e.

Suppose the quotient of a ring R is the field F. If $\mathcal{T}$ is any ring topology on F, then R is $\mathcal{T}$-discrete if and only if $\mathcal{T}_R \vee \mathcal{T} = \mathbf{1}$.

The following elementary observation will often be used here:

Theorem 1. *Suppose R is a subring of a nontrivial absolute valued field $(F, |\ |)$.*
(1) *R is discrete if and only if $\wedge |R^*| \geq 1$.*
(2) *If R is discrete, then each element invertible in R has absolute value one.*
(3) *If R is discrete and the quotient field of R is F, then R is unbounded.*

An obvious generalization of (1) above is the following: If $(R, \|\ \|)$ is a normed ring (as defined, e.g., in [3, Definition 5.1.1]) which has zero as its only algebraic nilpotent and which is discrete in its norm topology, then $\wedge \|R^*\| \geq 1$. This follows from the fact that an element with norm less than one is nilpotent.

Example 2. By checking each pair of elements to see that the norm requirements for sums and products are met, we see that a nonarchimedean norm is defined on $R = \mathbf{Z}/(4)$ if and only if $\|0\| = 0$ and $0 < \|2\|, 1 \leq \|1\| = \|3\|$. Note $2^2 = 0$. We have $\wedge \|R^*\| = \|2\|$, which may be less than 1.

The intersection of a compact subset and a closed discrete subset of a Hausdorff space is finite. Thus, a closed discrete subset of a σ-compact Hausdorff space is countable. Since a field with a nondiscrete locally compact ring topology is σ-compact (and has cardinality $\mathbf{c}$), discrete subrings (and their quotient fields) in locally compact fields are countable. Therefore, a necessary condition that a subfield K of a nondiscrete locally compact field have a discrete order is that K be countable. Discrete subrings of locally compact fields (viz., finite extensions of the p-adic fields, completions of function fields over a finite field, and $\mathbf{R}$ and $\mathbf{C}$) are considered further below.

Suppose R is a discrete subring of a field F with a real valued nonarchimedean valuation, $| \; |$, and x is an element in F with valuation at least one. If the multiplicative semigroup generated by $|x|$ and the multiplicative group generated by $|R^*|$ are disjoint, then $R[x]$ is discrete also. (The terms of a polynomial in x with coefficients in R will necessarily have distinct valuations, which implies the valuation of the sum is the maximum of the valuations of the terms.) For example, if K is a discrete subfield of an absolute valued field F and $x \in F$ has valuation greater than one, then $K[x]$ is discrete.

Similar reasoning (see Theorem 4 below) provides a partial answer to the following natural question: If R is a discrete subring of a topological ring E with identity 1, when will $R[1]$ (which equals $R + \mathbf{Z}$) be discrete? The proof of [4, Theorem 1] implicitly used the fact that this question has a positive answer when E is a field with an absolute value.

Lemma 3. *A topological ring E of pure characteristic with identity $e \neq 0$ has a discrete subring distinct from $\{0\}$ if and only if the ring of integers of E is discrete.*

Proof. If $\mathbf{Z}$ is not discrete and x is a nonzero element of a subring (or, more generally, any additive subsemigroup) R of E, then $\mathbf{Z}x$ is a nondiscrete subset of R. □

If E is a ring with identity $e \neq 0$ and with pure characteristic n, then n is prime or zero: If $n = mk$, where m and k are positive integers less than n, then m, viewed as an integer of E, has order k instead of the hypothesized value n. Thus, the ring $\mathbf{Z}$ of integers of E is an integral domain (and consequently 0 is the only algebraically nilpotent integer). Thus, if $\| \|$ is a norm on E with respect to which $\mathbf{Z}$ is discrete, then $\wedge \|\mathbf{Z}^*\| \geq 1$.

Theorem 4. (1) *If $R \neq \{0\}$ is a discrete subring of a normed integral domain $(E, \| \|)$ with identity, then $R[1]$ is discrete.*

(2) *If $R \neq \{0\}$ is a discrete subring of a nonarchimedean normed ring $(E, \| \|)$ of pure characteristic with identity and $\|R^*\| \cap \|\mathbf{Z}^*\| = \emptyset$, then $R[1]$ is discrete.*

Proof. (1) If $s \in R^*$ and $r + n \in (R + \mathbf{Z})^*$, where $r \in R$ and $n \in \mathbf{Z}$, then

$$1 \leq \|s(r + n)\| \leq \|s\| \|r + n\|.$$

By fixing s and letting r and n vary, we see that $(R + \mathbf{Z})^*$ is bounded away from zero.

(2) For r and n as in the proof of (1) above, either $r \neq 0$ or $n \neq 0$. By the disjointness hypothesis

$$\|r + n\| = \max(\|r\|, \|n\|) \geq (\wedge \|R^*\|) \wedge (\wedge \|\mathbf{Z}^*\|) > 0. \qquad \square$$

Example 5. In the ring $E = \mathbf{Z} \times \mathbf{Z}$ topologized by the norm $\|(a,b)\| = \max(|a|_p, |b|_1)$, where $|\ |_p$ is the p-adic absolute value and $|\ |_1$ is the trivial absolute value, the subring $\{0\} \times \mathbf{Z}$ and the ring $\mathbf{Z}(1,1)$ of integers of E are discrete, but the ring $(\{0\} \times \mathbf{Z})[1]$ (which is all of E) is not discrete.

By Zorn's lemma, every discrete subring of a field with an absolute value is contained in a maximal discrete subring. If R is a discrete subring of a field with an absolute value, then the quotient $U^{-1}R$ of R with respect to the semigroup U of elements in R with absolute value one is also a discrete ring, provided U is not empty. If R is a maximal discrete subring, then $R = \{0\}$ or $1 \in R$, by Theorem 4, which implies $U \neq \emptyset$. Therefore, an element in R is invertible if and only if the element has absolute value one.

Theorem 6. *The only discrete subring of a rank one valued extension of* $\mathbf{Q}$ *with a* p*-adic valuation is* $\{0\}$.

Conversely, if F *is a field with a nontrivial valuation* v *that is not an extension of* $\mathbf{Q}$ *with a* p*-adic valuation, then* F *contains an unbounded discrete unique factorization domain* R.

Proof. The first statement follows from Lemma 3.

Suppose (F, v) is not an extension of a p-adic valuation. If F is a subfield of $\mathbf{C}$ with a power of the usual absolute value, then we let $R = \mathbf{Z}$. Otherwise F is nonarchimedean and the prime subfield F_0 of F has trivial valuation. Let D consist of one element from each equivalence class of the following equivalence relation on the set of elements greater than one in the value group: $g, h \in v(F^*)$ are equivalent if there is a natural number n such that $g < h^n$ and $h < g^n$. If $A \subset F$ is such that $v|_A : A \longrightarrow D$ is bijective, then $R = F_0[A]$ is a discrete subring with a cofinal set of values. $\square$

Let M denote the function field $K(x)$ over an arbitrary field K, and let $|\ |$ denote the $(1/x)$-adic valuation of M. The power series field $K((1/x))$ is the completion $\hat{M}$ of M. For $u \in \hat{M} \backslash K$, $K[u]$ is a discrete subring of $\hat{M}$ if and only if $|u| > 1$. The previous discussion establishes the claim except when $|u| = 1$. If $|u| = 1$, then $u = \sum_{i \geq 0} a_i (1/x)^i$, $a_i \in K$, $a_0 \neq 0$. Thus, $-a_0 + u \in K[u]$, and $|-a_0 + u| < 1$.

The ring $K[x]$ is a maximal (but not the largest) discrete subring of $\hat{M}$: If u is an element in a discrete subring R containing $K[x]$ and u has series representation $\sum_N^\infty a_i (1/x)^i$, then we may write $u = f + d$, where f is (the polynomial which is) the sum of the terms in the representation with nonpositive index and d (with $|d| < 1$) is the sum of the terms with positive index. Since $d = u - f \in R$, we have $d = 0$ and $u = f \in K[x]$.

If R is a discrete subring of M and (when $K \cap R \neq \{0\}$) K_0 is the quotient field of $K \cap R$ in K, then $R[K_0] = ((K \cap R)^*)^{-1} R$ is a discrete ring.

Each maximal discrete subring R of M contains a subfield of K: $1 \in R$, so $K \cap R$ is a subring of R whose quotient is in R.

If u is an element of a commutative ring with identity, the subring generated by u is $u\mathbf{Z}[u] = \{\sum_{i\geq 1} n_i u^i : n_i \in \mathbf{Z}\}$, and $(u\mathbf{Z}[u])[1] = \mathbf{Z}[u]$.

Theorem 7. *Suppose $u \in \hat{M}\backslash K$ and $|u| = 1$. If u has canonical representation $u = \sum_{i=0}^{\infty} a_i(1/x)^i$, where each $a_i \in K$ and $a_0 \neq 0$, then the following are equivalent:*
(1) $u\mathbf{Z}[u]$ is discrete.
(2) $\mathbf{Z}[u]$ is discrete.
(3) a_0 is not algebraic over the prime subfield of K.

Proof. Since $\mathbf{Z}[u]$ and $u\mathbf{Z}[u]$ are homeomorphic, (1) and (2) are equivalent. Now $\mathbf{Z}[u]$ is discrete if and only if each sum $\sum_{i\leq k} n_i u^i$, with $n_i \in \mathbf{Z}$ and $n_k \neq 0$, has valuation greater than or equal to one. Let $d = u - a_0$, and note $|d| < 1$. Use the binomial theorem and collect the highest powers of a_0 in each binomial expansion to obtain that

$$\sum n_i u^i = \sum n_i (a_0 + d)^i = (\sum n_i a_0^i) + dy,$$

where $|y| \leq 1$. Therefore, $|\sum n_i u^i| < 1$ if and only if $\sum n_i a_0^i = 0$. □

Suppose $u \in M$ and $u = f/g$, where f and g are relatively prime polynomials in $K[x]$. Since $|u| = 1$, f and g have the same degree, say n. Let f_i and g_i be the coefficients of x^i in f and g, respectively. By "long division", we see that $a_0 = f_n/g_n$.

Corollary 8. *If K is algebraic over its prime subfield (as is the case if M has locally compact completion) and R is a discrete subring of $\hat{M}$, then $|u| > 1$ for each element $u \in R\backslash K$.*

Proof. If K is algebraic over its prime field and R is a discrete subring of M and $u \in R\backslash K$, then the ring generated by u (which is contained in R) is discrete. Therefore, $|u| > 1$. □

We consider discrete subrings of the real and complex numbers.

Lemma 9. *If R is a subring of an integral domain E, $a \in E$, the identity of E is in R, and Ra is a ring, then $a \in R$.*

Proof. Since $a^2 = ra$ for some $r \in R$, we have $a = r \in R$. □

Theorem 10. *In $(\mathbf{Q}, |\ |_\infty)$ the ideals $n\mathbf{Z}$, $n \in \mathbf{Z}$, are discrete. Conversely, every discrete subring of $(\mathbf{R}, |\ |_\infty)$ is an ideal of $\mathbf{Z}$.*

Thus, $\mathbf{Q}$ is the only subfield of $\mathbf{R}$ with a discrete order.

Proof. Let R be a nonzero discrete additive subgroup of the real numbers $\mathbf{R}$. Then R is cyclic (i.e., $R = \mathbf{Z}a$, for some $a \in \mathbf{R}$) rather than dense. If $\mathbf{Z}a$ is a ring, then $a \in \mathbf{Z}$. □

Observe that a discrete subgroup of $\mathbf{C}$ will have finite intersection with any bounded set.

Lemma 11. *Suppose $L = \mathbf{Z}u + \mathbf{Z}v$, where u and v are complex numbers. For each $x \in L^*$, the set $(\mathbf{Q}x) \cap L^*$ has an element w with minimum absolute value. For such an element w, $L = \mathbf{Z}w + \mathbf{Z}y$ for some $y \in L$.*

Proof. *Case* 1: u and v are linearly independent over $\mathbf{Q}$. Let $x = m'u + n'v$, where m' and n' are integers with greatest common divisor g and let $m = m'/g$ and $n = n'/g$. Let

$$w := \frac{1}{g}x = mu + nv \in (\mathbf{Q}x) \cap L^*.$$

We show $|w|$ is minimal in $|(\mathbf{Q}x) \cap L^*|$: Given

$$\frac{c}{d}x = ku + lv \in (\mathbf{Q}x) \cap L^*$$

(where $c, d, k, l \in \mathbf{Z}$), we equate coefficients to obtain

$$\frac{c}{d}m' = k \qquad \text{and} \qquad \frac{c}{d}n' = l; \qquad \frac{m}{n} = \frac{m'}{n'} = \frac{k}{l}.$$

Since m and n are relatively prime, there is an integer j such that $k = jm$ and $l = jn$. Therefore, $|ku + lv| = |jw| \geq |w|$.

There are integers a and b such that $am + bn = 1$. Thus, the determinant with respect to the ordered basis u, v of the $\mathbf{Z}$-linear map $A : L \longrightarrow L$ determined by

$$Au = w, \qquad Av = -bu + av$$

equals one, so $L = \mathbf{Z}w + \mathbf{Z}(-bu + av)$.

Case 2: $u = v = 0$. Then $L^* = \emptyset$ and the theorem is vacuously true.

Case 3: Exactly one of u and v is zero. Then we may choose w to be the nonzero one and y to be 0.

Case 4: u and v are dependent over $\mathbf{Q}$, but neither is zero. Then $mu = nv$ for some rational m and n, and, by multiplying both sides by an appropriate integer, we assume m and n are relatively prime integers. Let $t = mu (= nv)$, and let $am + bn = 1$ for integers a and b. Then

$$bu + av = b\frac{t}{m} + a\frac{t}{n} = \frac{(bn + am)t}{mn} = \frac{t}{mn} \in L.$$

Conversely, if $x = cu + dv \in L$, then

$$x = \frac{cn(mu) + dm(nv)}{mn} = (cn + dm)\frac{t}{mn}.$$

Thus, $L = \mathbf{Z}(t/mn)$, so we may let $w = t/mn$ and $y = 0$. $\square$

Theorem 12. *A discrete subring R of the complex numbers which contains a nonzero real number, but which is not contained in the reals, is of the form $R = \mathbf{Z}u + \mathbf{Z}v$, where u is an integer and v satisfies the equations*

$$\begin{aligned} v &= \frac{b+\sqrt{b^2+4au}}{2}, \\ v^2 &= au + bv \end{aligned}$$

for some integers a and b such that

$$au < 0, \qquad |b| < 2\sqrt{-au}.$$

Conversely, if u, a and b are integers satisfying the inequalities above and v is defined by the first equality displayed above, then $\mathbf{Z}u + \mathbf{Z}v$ is a discrete ring and the second equality displayed above is also satisfied.

Proof. A discrete additive subgroup R of the complex numbers is of the form $\mathbf{Z}u$ or $\mathbf{Z}u + \mathbf{Z}v$, where u and v are linearly independent over the real numbers (see, e.g., [1, p. 150]). If R is a ring and $R = \mathbf{Z}u$, then, by Lemma 9, $u \in \mathbf{Z}$ and $R \subset \mathbf{R}$. Therefore, if R is as in the statement of the theorem, $R = \mathbf{Z}u + \mathbf{Z}v$, where (by Lemma 11) we may assume u is real. Since $u^2 \in R$, $u^2 = mu + nv$ for some integers m and n. In fact $n = 0$, because $nv = u^2 - mu \in \mathbf{R}$. Thus, $u = u^2/u = mu/u \in \mathbf{Z}$. Since $v^2 \in R$, $v^2 = au+bv$ for some integers a and b. Applying the quadratic formula to this equation in v and taking into account that v is not real completes the proof of the first statement of the theorem. (If v is the solution to the quadratic with minus the radical, then note $R = \mathbf{Z}u + \mathbf{Z}(-v)$ and

$$\begin{aligned} (-v)^2 &= v^2 = au + bv = au + (-b)(-v), \\ -v &= \frac{-b+\sqrt{b^2+4au}}{2} = \frac{(-b)+\sqrt{(-b)^2+4au}}{2}; \end{aligned}$$

so we may replace v by $-v$ in the argument.)

To prove the converse let $R = \mathbf{Z}u + \mathbf{Z}v$. Then R is an additive group; R is a ring (i.e., it is also closed under multiplication) if and only if $u^2, v^2, uv \in R$. For u and v as described in the theorem u^2 and uv are obviously in R and $v^2 = au + bv \in R$ because v has been defined to be a root of this equation. $\square$

Corollary 13. *A subfield K (with the relative topology) of the complex numbers with the usual topology contains a discrete order if and only if $K = \mathbf{Q}$ or $[K : \mathbf{Q}] = 2$ and $K \not\subset \mathbf{R}$.*

The discrete subrings of $\mathbf{C}$ with the most symmetry properties as lattices (in the crystallographic sense) are the rectangular lattices $\mathbf{Z}[\sqrt{-n}]$, $n \in \mathbf{Z}_{>0}$ (obtained in Theorem 12 by letting $u = 1$, $a = -n$, and $b = 0$) and the hexagonal lattice $\mathbf{Z}[e^{\pi i/3}]$ (the ring generated by the sixth roots of unity; obtained in Theorem 12 by letting $u = -a = b = 1$). Since $\mathbf{Z}[\sqrt{-3}]$ is a standard example of a ring in which factorization is not unique [$4 = 2^2 = (1 + \sqrt{-3})(1 - \sqrt{-3})$], we see that a discrete subring of a nontrivial absolute valued field may not be a unique factorization domain.

Acknowledgements

The author thanks the referee for making several corrections and improvements.

References

[1] E. Artin, Theory of algebraic numbers, Göttinger, 1959.
[2] N. Shell, Maximal and minimal ring topologies, Proc. Amer. Math. Soc. 68 (1978) 23–26.
[3] N. Shell, Topological Fields and Near Valuations, Vol. 135 (Dekker, New York, 1990).
[4] N. Shell, Residue class topologies, Conference on General Topology and Applications, Queens College, Flushing, 1993, Lecture Notes in Pure and Applied Mathematics (Dekker, New York, 1995).
[5] N. Shell, Direct topologies from discrete rings, Conference on General Topology and Applications, Univ. Southern Maine, 1995, to appear.
[6] N. Shell, Direct topologies from discrete rings, II, to appear.