

FINITE INDEX CONDITIONS IN RINGS

CHARLES LANSKI

ABSTRACT. This paper determines the structure of an associative ring R when either all of its additive subgroups, all of its subrings, all of its (right) ideals, or all of its Lie ideals have finite additive index in R .

There are a number of results in the literature that impose finiteness conditions on certain subsets or substructures of rings to study consequent restrictions on the structure of the ring (e.g., [1, 2, 5–7, 9–13]).

The work here was motivated by a result about infinite groups in which each nonidentity subgroup has finite index [1]. It is immediate that an infinite cyclic group satisfies this property. The converse, that an infinite group must be cyclic if every nonidentity subgroup has finite index, is not obvious but was proved by Fedorov [1] using rather sophisticated group theoretic ideas and results (see [11] for an elementary proof). Is there a corresponding result for rings? Of course, to consider any quotient R/S of a ring R , S must be an additive subgroup of R . The usual kinds of additive subgroups that one might consider in a ring R are the additive subgroups themselves, subrings, one-sided ideals, ideals and perhaps Lie ideals. Our purpose here is to study, for each of these types of substructures, what restrictions on R result if all nonzero such have finite additive index in R .

The result of Fedorov [1] is crucial for our results, and we state it here for reference.

Theorem A. If all nonidentity subgroups of an infinite group G have finite index, then G is cyclic.

2010 AMS *Mathematics subject classification.* Primary 16D25, 16D70, 16P70, 16W10.

Received by the editors on June 24, 2013.

DOI:10.1216/RMJ-2015-45-4-1177

Copyright ©2015 Rocky Mountain Mathematics Consortium

For the following discussion, we assume that R is an infinite ring. Clearly, for $m \geq 1$ if $R \cong m\mathbb{Z}$ as rings, or if $R^2 = (0)$ with $(R, +) \cong (\mathbb{Z}, +)$, then the quotient $(R, +)/S$ is finite for any nonzero additive subgroup S . Let us call these the *standard examples*. The strongest assumption we can make, and the exact analogue of Theorem A, is to assume that R/A is finite, as an additive group, for all nonzero additive subgroups A of R . In this case, the ring structure of R follows easily from its additive structure given by Theorem A, and must be a standard example.

Our main result (Theorem 4), which is the closest natural analogue of Theorem A for rings, assumes the finiteness of R/S for all nonzero subrings S of R . Surprisingly, this assumption yields the same characterization of R as for the additive subgroup case—the standard examples, but is considerably more difficult to prove.

By assuming the finite index condition for other ring theoretic structures we can obtain only necessary conditions on R , not characterizations. The weakest assumption we can make is that all nonzero ideals of R have finite quotients. We can show in this case (Theorem 1) that R is a standard example or R must be prime. Of course, all simple rings satisfy this condition. Also, any prime ring R containing an ideal M that is a simple ring so that R/M is finite satisfies the finite index condition for ideals. Examples of such rings, and other examples, are provided after Theorem 1. The finite index condition for right ideals (Theorem 3) implies that R is a standard example or an Ore domain. Finally, the finite index condition for Lie ideals (Theorem 5) leads to a description for R similar to that for ideals, but examples of such rings are more difficult to find. It is particularly interesting that in all of these cases either R has trivial multiplication or R is a prime ring.

For any additive subgroup A of a ring R we denote the index of A in R , as additive groups, by $[R : A]$. For any $x \in R$, we let $\langle x \rangle$ denote the additive subgroup generated by x . Our first theorem, for ideals, gives an important dichotomy for the structure of R that will be used in our subsequent results.

Theorem 1. *If R is an infinite ring so that $[R : I]$ is finite for every nonzero ideal I of R , then $R^2 = (0)$ and $(R, +) \cong (\mathbb{Z}, +)$, or R is a prime ring. If R is prime and is an algebra over an infinite field, then R must be a simple ring.*

Proof. If $R^2 = (0)$, then every additive subgroup of R is an ideal of R , so applying Theorem A yields $(R, +) \cong (\mathbb{Z}, +)$. Otherwise, let $\text{Ann}(R)$ be the two-sided annihilator of R , a proper ideal of R . Assume first that $\text{Ann}(R) \neq (0)$. Using $R/\text{Ann}(R)$ finite, let

$$R = \bigcup (\text{Ann}(R) + r_j) \quad \text{for } \{r_1, \dots, r_t\} \subset R.$$

If $R^3 \neq (0)$, then there is $x \in R$ with RxR a nonzero ideal of R . Since $x\text{Ann}(R) = \text{Ann}(R)x = (0)$, it follows that RxR is generated as an additive group by $\{r_j x r_i \mid 1 \leq i, j \leq t\}$, a finite set. Now, if $R/\text{Ann}(R)$ has order $v > 1$ as a finite nonzero additive group, then $vR \subseteq \text{Ann}(R)$. Therefore, all $vr_j x r_i = (vr_j) x r_i = 0$ so RxR is a finite nonzero ideal. This, together with our assumption that R/RxR is finite, results in R finite, a contradiction. Thus, we may assume that $R^3 = (0)$ when $\text{Ann}(R) \neq (0)$.

We are assuming that $R^2 \neq (0)$, so it is a proper nonzero ideal of R . Thus, R/R^2 is finite, and so there is an integer $w > 0$ with $wR \subseteq R^2$. Further, for some $\{0 = t_1, t_2, \dots, t_k\} \subseteq R$, with $k \geq 2$, we have

$$R = \bigcup (R^2 + t_j).$$

Therefore, any $r \in R$ can be written as $r = x + t_j$ for some $x \in R^2$ and some $1 \leq j \leq k$. Since $R^3 = (0)$ but $R^2 \neq (0)$, there is some $0 \neq y = t_i t_j \in R^2$. It follows that $y \in \text{Ann}(R)$ and that $wy = (wt_i)t_j \in R^2 R = (0)$, so $\langle y \rangle$ is a finite ideal of R . Using that $R/\langle y \rangle$ is finite yields the contradiction that R is finite. Consequently, $\text{Ann}(R) \neq 0$ forces $R^2 = (0)$ and $(R, +) \cong (\mathbb{Z}, +)$, and we may now assume that $\text{Ann}(R) = (0)$.

Let N be a nonzero nilpotent ideal of R with $N^m = (0)$ for $m > 1$ and minimal. We proceed much as above. Now N^{m-1} is a nonzero ideal of R so R/N^{m-1} is finite, and there is an integer $v > 1$ with $vR \subseteq N^{m-1}$ and also some $\{s_1, \dots, s_q\} \subseteq R$ so that

$$R = \bigcup (N^{m-1} + s_j).$$

Hence, $(vN)R = N(vR) = (0) = (vR)N = R(vN)$. This shows first that $vN \subseteq \text{Ann}(R) = (0)$, and then that $v^2 R = v(vR) \subseteq vN^{m-1} = (0)$. Let $0 \neq y \in N$, and let I be the ideal of R generated by y . Thus, $I = \langle y \rangle + Ry + yR + RyR$ is generated as an additive subgroup by the finite set $\{y, ys_i, s_j y, s_j y s_i \mid 1 \leq i, j \leq q\}$, using that $R = \bigcup (N^{m-1} + s_j)$.

But $v^2R = (0)$, so I is a nonzero finite ideal, and once again this forces the contradiction that R is finite. Hence, if $\text{Ann}(R) = (0)$, then R cannot have a nonzero nilpotent ideal.

Finally, if I and J are nonzero ideals of R then R/I and R/J are finite, and so $R/(I \cap J)$ embeds isomorphically into the finite ring $R/I \oplus R/J$ via $r \mapsto (I + r, J + r)$. Thus, $I \cap J \neq (0)$, since otherwise R would be finite. But $(I \cap J)^2 \subseteq IJ$, and since R has no nonzero nilpotent ideals, we are forced to conclude that $IJ \neq (0)$, proving that R must be a prime ring. Now assume that R is a prime algebra over the infinite field F and has a proper nonzero ideal I . Then IR is a proper nonzero algebra ideal of R , so R/IR is an algebra over F and, by our assumption, is a nonzero finite ring. This obvious contradiction shows that R must be a simple ring. This completes the proof of the theorem. \square

Aside from the standard examples, what are some nonsimple infinite prime rings R for which R/I is finite for all nonzero ideals I ? A commutative domain of characteristic zero with this property is $\mathbb{Z}[\sqrt{-5}]$, and many others can be obtained by replacing -5 with other integers or suitable integral elements in the complex numbers. The idea here is that the ideal I of $\mathbb{Z}[\sqrt{-5}]$ generated by any nonzero element α contains $m\mathbb{Z}$ for m the norm of α , so $\text{card } R/I \leq m^2$. These examples show that R need not be a PID or a UFD. To get examples when $\text{char } R = p$, a prime, let F be a finite field with $\text{char } F = p$. Since $F[x]$ is a PID, it is easy to see that $F[x]$ and $F[x^2, x^3]$ are examples. Similarly the power series ring $F[[x]]$ is an uncountable PID with all proper quotients finite, since any proper, nonzero ideal is generated by a power of x . The last three examples give rise to noncommutative versions

$$F[x; \phi], \quad F[x^2, x^3; \phi], \quad \text{and} \quad F[[x; \phi]]$$

for ϕ a nonidentity automorphism ϕ of F , by twisting the scalar multiplication via $x^k f = \phi(x)^k (f) x^k$ for $f \in F$. Just as for the commutative ring $F[x]$, if I is a nonzero ideal, or right ideal, of $F[x; \phi]$ and if $0 \neq g(x) \in I$ has minimal degree, say n , then every $f(x) \in F[x; \phi]$ has the form

$$f(x) = h(x) + p(x)$$

for $h(x) \in I$ and $\deg p(x) < n$. Consequently, $F[x; \phi]/I$ has at most $(\text{card } F)^n$ elements. Similar considerations hold for $F[x^2, x^3; \phi]$

and $F[[x; \phi]]$; in the latter case, because each nonzero (right) ideal is generated by a power of x , as for $F[[x]]$.

An example of a noncommutative domain of characteristic zero with all nonzero ideals of finite index is the ring of quaternions over the integers. That is, if \mathfrak{Q} is the division ring of real quaternions, then let $R = \{a + bi + cj + dk \in \mathfrak{Q} \mid a, b, c, d \in \mathbb{Z}\}$. Clearly, R is a noncommutative domain and R/I is finite for every nonzero ideal I . To see the latter, for $0 \neq \alpha = a + bi + cj + dk \in I$, its norm, the product of α with $a - bi - cj - dk$, is $a^2 + b^2 + c^2 + d^2$, so I contains the quaternions over some nonzero ideal of \mathbb{Z} . This forces the quotient ring R/I to be a finite module over the ring of integers modulo the norm of α : $|R/I| \leq (\text{norm}(\alpha))^4$.

Let A represent any of the examples above that have an identity element. For any ring R with identity element each ideal in the matrix ring $M_n(R)$ is just $M_n(J)$ for J an ideal of R . Thus, matrix rings $M_n(A)$ are examples: nonsimple rings with zero divisors and nilpotent elements having every proper quotient finite.

More generally, if J is a nonzero ideal of A , then any subring $S \subseteq M_n(A)$ that contains $M_n(J)$ is an example. The reason is that any nonzero ideal W of S contains the ideal $M_n(JaJ)$ for any nonzero entry a of any element of W ; this forces S/W to be finite by the choice of A . It follows that $M_n(J)$ itself is an example without an identity element. Similarly, matrices over the ring $m\mathbb{Z}$ yield examples without identity elements and having all proper quotients finite.

We present characteristic p examples that are finite extensions of simple rings, as mentioned in the introduction. These require a bit of notation.

Example 1. Let K be a field, V a countably infinite dimensional vector space over K , and consider $\text{Hom}_K V$ to be the row (or column) finite, countable by countable matrices over K . Denote by $M_0(K)$ the subring of $\text{Hom}_K V$ consisting of all matrices with only finitely many nonzero entries. It is straightforward to show that $M_0(K)$ is a simple ring by using the standard matrix units in $M_0(K)$. When $\text{char } K = p > 0$, then for any fixed integer $n > 1$ and any finite subfield F of K , choose a nonzero subring $S \subseteq M_n(F)$. Now let R be the subring of $\text{Hom}_K V$ generated by $M_0(K)$ and all $n \times n$ block diagonal matrices that have a

fixed $A \in S$ for all $n \times n$ diagonal blocks—the $n \times n$ block matrices with A in the upper left corner and repeated consecutively and countably infinitely down the diagonal. Then $M_0(K)$ is the unique minimal ideal of R and $R/M_0(K) \cong S$, which is finite. Hence, if I is any nonzero ideal of R , then R/I is finite. Further, these examples can be extended naturally to the case when $\dim_K V$ has arbitrary infinite cardinality. Thus, there are examples R for Theorem 1 that are uncountable, and of arbitrary infinite cardinality.

In Example 1, although K with $\text{char } K = p$ may be infinite, those $R \neq M_0(K)$ are not algebras over K but only over the finite field F : K is the extended centroid of R . In Example 1 with V infinite dimensional over K , when S contains the identity matrix $I_n \in M_n(F)$, then R has an identity element and FI_R is the center of R . However, no similar example, having a simple ideal, exists if $\text{char } R = 0$. That is, if a prime ring R satisfies the property that R/I is finite for all nonzero ideals I , if R has a nonzero ideal M that is a simple ring, and if $\text{char } R = 0$, then $R = M$. For, if $y \in R - M$, then R/M finite implies that $\{M + ky \mid k \in \mathbb{Z}\} \subseteq R/M$ is finite. It follows that $ny \in M$ for an integer $n > 1$. Since M is simple and torsion free, $nM = M$, so for some $x \in M, ny = nx$. Now R torsion free forces $y = x \in M$. Consequently, any such R must be a simple ring.

We show next that the same assumption as in Theorem A gives a similar result for rings: R must be a standard example. The argument is quite easy. Recall that, for $y \in R$, the additive subgroup of R generated by y is $\langle y \rangle$.

Theorem 2. *If R is an infinite ring so that $[R:A]$ is finite for every nonzero additive subgroup A of R , then $(R, +) \cong (\mathbb{Z}, +)$ and as a ring $R^2 = (0)$ or $R \cong m\mathbb{Z}$ for some $m \geq 1$.*

Proof. A direct application of Theorem A shows that $(R, +) \cong (\mathbb{Z}, +)$. Consequently, if $(R, +) = \langle y \rangle$, then the ring structure of R is determined by $y^2 = my \in \langle y \rangle$ for an integer m . When $m = 0, R^2 = (0)$, suppose that $m \geq 1$. It is clear that, for an indeterminate x over \mathbb{Z} , $R \cong x\mathbb{Z}[x]/(x^2 - mx)$ as rings. Let $g: x\mathbb{Z}[x] \rightarrow m\mathbb{Z}$ be given by $g(p(x)) = p(m)$. Now g is a surjective homomorphism of rings with $\ker g = (x^2 - mx)$, since these are the polynomials divisible by both

x and $x - m$. Thus, $R \cong m\mathbb{Z}$ as rings. When $m < 0$, then using $\langle -y \rangle = \langle y \rangle$ and then $(-y)^2 = y^2 = my = (-m)(-y)$, we get again that $R \cong (-m)\mathbb{Z}$ as rings. \square

We next consider the structure of a ring R so that the quotient of R by any nonzero right ideal is finite as an additive group. With this assumption, it is immediate that R is a right Noetherian ring. What infinite rings have this finite index property for right ideals? Clearly, the standard examples and the domains presented after Theorem 1 do, but the matrix examples over those domains do not. The example $F[x^2, x^3]$ shows that R need not be a PID, or a UFD. Are there examples with zero divisors?

Our next result has the same kind of dichotomy as in Theorem 1 but the stronger hypothesis about right ideals yields a bit more information about the structure of R : it is a domain or is $(\mathbb{Z}, +)$ with trivial multiplication.

Theorem 3. *Let R be an infinite ring so that, for each nonzero right ideal T , the index $[R: T]$ as an additive group is finite. Then R is a division ring, R is a right Noetherian Ore domain with every proper, nonzero, prime ideal maximal, or $R^2 = (0)$ and $(R, +) \cong (\mathbb{Z}, +)$. Furthermore, if R is a simple domain, then R must be a division ring.*

Proof. Our hypothesis shows immediately that R must be a right Noetherian ring. Since every nonzero ideal of R is a right ideal we may apply Theorem 1 and conclude that R is prime or $R^2 = (0)$ and $(R, +) \cong (\mathbb{Z}, +)$. Thus, we may assume that R is a prime ring. Suppose that, for nonzero $a, b \in R$, $ab = 0$. Hence, $r(a)$, the right annihilator of a , is a proper nonzero right ideal. Note that $aR \neq (0)$ since R is prime. The map $\phi: R \rightarrow aR$ via $\phi(r) = ar$ is a surjective R -module homomorphism with kernel $r(a)$. Since $r(a) \neq (0)$ and $aR \cong R/r(a)$, we must have aR finite, and its quotient R/aR is finite by assumption, forcing the contradiction that R is finite. This proves that R must be a right Noetherian domain, from which it follows that R must be an Ore domain. It is simple to see this directly in our situation. If, for nonzero right ideals T and S of R , we had $T \cap S = (0)$, then R would embed isomorphically in the finite additive group $R/T \oplus R/S$, contradicting R infinite. Hence, R must be an Ore domain.

Next, if I is any proper, nonzero, prime ideal of R , then R/I is a finite prime ring, so a simple ring, forcing I to be a maximal ideal of R .

Finally, suppose that R is an infinite, simple domain but not a division ring, so R contains a proper nonzero right ideal T . Using that R/T is finite, $R = \bigcup(T + x_j)$ for a finite $\{x_1, \dots, x_k\} \subseteq R$, where no $x_j = 0$ and some $x_i \in T$. Since R is a domain, $x_j R$ is infinite for each j . Using that R is an Ore domain shows first that, for each j ,

$$T \cap x_j R \neq (0),$$

so

$$W(x_j) = \{y \in R \mid x_j y \in T\}$$

is a nonzero right ideal of R , and then that

$$W = \bigcap W(x_j)$$

is a nonzero right ideal of R . But now, since R is simple,

$$R = RW = \bigcup(T + x_j)W \subseteq T.$$

This contradiction shows that R must be a division ring, completing the proof of the theorem. \square

Since in a commutative ring every right ideal is an ideal, examples of infinite commutative rings satisfying the finite index condition in Theorem 3 are the examples given after Theorem 1. As mentioned after Theorem 1, the twisted polynomial rings

$$F[x; \phi] \quad \text{and} \quad F[x^2, x^3; \phi],$$

and the twisted power series ring $F[[x; \phi]]$, all over a finite field F , satisfy the finite index condition on right ideals. An example in characteristic zero is the ring R of quaternions over the integers, also discussed after Theorem 1. Just as mentioned there, any nonzero right ideal T contains the norm of each of its elements, so it contains an ideal mR for some nonzero $m \in \mathbb{Z}$. Thus,

$$[R : T] \leq m^4.$$

Using Theorem 3, we can obtain our main result, the natural ring theoretic analogue of Theorem A that assumes all nonzero subrings

of R have finite index. The conclusion for infinite rings is the same characterization as in Theorem 2: the ring must be $m\mathbb{Z}$ or the additive group of integers with trivial multiplication. Our argument requires a certain fact that we prove first. In any ring R let $[y]$ denote the subring of R generated by $y \in R$.

Lemma 1. *Let R be a ring with 1_R , $\text{char } R = 0$ and with the property that each nonzero subring has finite additive index in R . Then $y \notin [1_R]$ forces $1_R \notin \mathbb{Z}y = \langle y \rangle$.*

Proof. We obtain a contradiction to the finite index condition for subrings by assuming that there is

$$y \notin [1_R] \quad \text{with } ny = 1_R$$

for some integer n . Should $n < 0$, then replace y with $-y \notin [1_R]$, and now $(-n)(-y) = 1_R$. Thus, we may assume that $ny = 1_R$ for a minimal positive integer $n > 1$. It follows that

$$[1_R] \subseteq [y].$$

Since $R/[1_R]$ is finite, the set of cosets $\{[1_R] + y^j \mid j > 0\}$ is finite, so there are positive integers $t > s$ with $y^t - y^s = m1_R$ for some integer m . Thus,

$$y = n^{t-1}y^t = n^{t-1}(m1_R + y^s) = n^{t-1}m1_R + n^{t-1-s}1_R \in [1_R].$$

This contradiction proves the lemma. \square

Theorem 4. *Let R be an infinite ring so that for every nonzero subring S , the index $[R: S]$ of $(S, +)$ in $(R, +)$ is finite. Then $(R, +) \cong (\mathbb{Z}, +)$ and either for some integer $m \geq 1$, $R \cong m\mathbb{Z}$ as rings, or $R^2 = (0)$.*

Proof. Since any right ideal of R is a subring of R we may apply Theorem 3 to conclude that $R^2 = (0)$ and $(R, +) \cong (\mathbb{Z}, +)$, or else R is a domain. Thus, we may assume that R is a domain. Note that the only idempotents in R can be 0 or 1_R , if R has an identity element. As above let $[x]$ denote the subring generated by $x \in R$. Should $[x]$ be finite for some $x \neq 0$, then

$$(R, +)/([x], +)$$

finite forces the contradiction that R is finite, so nonzero elements of R generate infinite subrings. Next assume that, for some nonzero $x \in R$, $[x] = [x^2]$. Since $x \in [x^2]$, for some polynomial $q(Y) \in \mathbb{Z}[Y]$,

$$x = x^2q(x^2);$$

let $e = xq(x^2) \in R$, and observe that $e^2 = e$ is an idempotent. If $e = 0$, then also $x = xe = 0$. Thus, when $x \neq 0$, $[x] = [x^2]$ implies that

$$1_R \in R \quad \text{and} \quad 1_R \in [x].$$

Since we are assuming that R is a domain, consider first when $\text{char } R = p > 0$, so R is an algebra over F_p , the field of p elements. We have seen that, for any $x \in R - \{0\}$, $[x]$ must be infinite. But, if R has an identity element 1_R , then $[1_R]$ would be finite, so R cannot have an identity element. Thus, as we saw above, if $x \in R - \{0\}$, then

$$[x] \neq [x^2].$$

In $[x]/[x^2]$, the subset

$$\{[x^2] + x^{2k-1} \mid k \geq 1\}$$

must be finite, so for some $k < t$,

$$x^{2t-1} - x^{2k-1} \in [x^2].$$

Consequently, x satisfies some nonzero polynomial over F_p . Since R is a domain, we may, if necessary, cancel powers of x to assume that $x = x^2g(x)$ for some nonzero $g(Y) \in F_p[Y]$. As above, this leads to a nontrivial idempotent in R , another contradiction. Therefore, it is not possible that $\text{char } R = p$.

We may now assume that $\text{char } R = 0$. Since R and its subrings are torsion free \mathbb{Z} algebras, if R has an identity element 1_R , then

$$[1_R] = \{k1_R \mid k \in \mathbb{Z}\} \cong \mathbb{Z}$$

as rings. Suppose there is some $y \in R - [1_R]$. Since $R/[1_R]$ is a finite additive group, its subset

$$\{[1_R] + ky \mid k \in \mathbb{Z}\}$$

is finite. Consequently, there are integers $t > s > 0$ so that $(t - s)y \in [1_R]$. Then

$$A = \{n \in \mathbb{Z} \mid ny \in [1_R]\} \neq (0)$$

is an additive subgroup of the integers, so $A = m\mathbb{Z}$ for $m > 1$ the smallest positive integer in A . We conclude from Lemma 1 that $my \neq \pm 1_R$.

Suppose $my = v1_R \in [1_R]$. If $v = 0$, then since R is torsion free, $y = 0$, contradicting its choice, so

$$v \neq 0 \quad \text{and} \quad |v| > 1.$$

If the integers m and v have a common factor $d > 1$, say $m = dw$ and $v = dz$, then

$$d1_R(wy - z1_R) = d(wy - z1_R) = 0,$$

so R torsion free forces $wy = z1_R$. Thus,

$$|w| \in A \quad \text{with} \quad |w| < m,$$

contradicting the minimality of m . The result is that

$$\text{GCD}(\{m, v\}) = 1.$$

Assume that $k > 1$ and $y^k \in [1_R]$. Then

$$v^{k-1}y = m^{k-1}y^k \in [1_R],$$

so $v^{k-1} \in A$, contradicting $\text{GCD}(\{m, v\}) = 1$. Just as above, since $y^k \notin [1_R]$, there is $A_k = \{n \in \mathbb{Z} \mid ny^k \in [1_R]\} = m_k\mathbb{Z}$ for some $m_k > 1$, using Lemma 1. Now $m^k \in A_k = m_k\mathbb{Z}$, so $m_k \mid m^k$. Also, as above, $m_k y^k = w1_R \in [1_R] - (0)$. It follows that

$$m^k w1_R = m_k m^k y^k = m_k v^k 1_R$$

and, by unique factorization in $[1_R] \cong \mathbb{Z}$, we have that m^k must divide m_k , forcing $m_k = m^k$. That is,

$$A_k = m^k\mathbb{Z}.$$

In particular,

$$\{[1_R] + y^k, [1_R] + 2y^k, \dots, [1_R] + m^k y^k\}$$

is a subset of distinct elements in the additive group $R/[1_R]$. But, if $\text{card } R/[1_R] = t$ and if $m^k > t$, we arrive at a contradiction. Therefore, we must conclude that there is no $y \in R - [1_R]$: that $R = [1_R] \cong \mathbb{Z}$.

Finally, we consider when R is a torsion free domain without an identity element. For any nonzero $x, y \in R$, since $R/[x]$ is finite, either

$y \in [x]$ and $xy = yx$, or else in $R/[x]$, $\{[x] + my \mid m > 0\}$ must be a finite set of cosets. Thus, there is an integer $n > 0$ so that $ny \in [x]$, and it follows that

$$n(yx) = (ny)x = x(ny) = n(xy).$$

But R torsion free means $xy = yx$, proving that R must be commutative. Further, from above, $[x] \neq [x^2]$ when $x \neq 0$. Therefore, $R/[x^2]$ finite shows that the set of cosets $\{[x^2] + mx \mid m > 0\}$ is finite, resulting in

$$nx = x^2q(x^2)$$

for some $n > 0$ and $q(Y) \in \mathbb{Z}[Y]$.

Since R is a torsion free \mathbb{Z} module, there is a ring isomorphism from \mathbb{Z} to a subring of $\text{End}((R, +))$ via left multiplication: the image $z^\#$ of $z \in \mathbb{Z}$ is given by

$$z^\#(r) = zr = r^z \in (R, +).$$

Similarly, left multiplication by $a \in R$ gives

$$a^\# \in \text{End}((R, +))$$

via $a^\#(r) = ar$. Our assumptions on R show that all of these $z^\#$ and $a^\#$ are injective maps and that

$$\#: R \longrightarrow \#(R) = R^\# \subseteq \text{End}((R, +)),$$

and

$$\#: \mathbb{Z} \longrightarrow \{z^\# \mid z \in \mathbb{Z}\} = \mathbb{Z}^\# \subseteq \text{End}((R, +))$$

are isomorphisms of rings. A direct computation shows that

$$za^\# = (za)^\# = z^\#a^\# = a^\#z^\#.$$

Therefore, if W is the subring of $\text{End}((R, +))$ generated by the images

$$\mathbb{Z}^\# \quad \text{and} \quad R^\#,$$

then W is a torsion free \mathbb{Z} module via multiplication by $\mathbb{Z}^\#$, and W is a commutative ring with identity $1^\#$. A typical element of W can be expressed as $z^\# + a^\#$ for some

$$z \in \mathbb{Z} \quad \text{and} \quad a \in R,$$

and $R^\# \cong R$ as rings, is an ideal of W . We show that nonzero subrings of W have finite index.

Suppose some $z^\# + a^\# \in W$ is not injective. Then, for some nonzero $b \in R$,

$$0 = (z^\# + a^\#)(b) = zb + ab.$$

Thus, for any $r \in R$,

$$0 = zrb + arb,$$

using that R is commutative, so R a domain yields $(z^\# + a^\#)(r) = 0$ for all $r \in R$, which means $z^\# + a^\# = 0$. Hence, each $0 \neq w \in W$ is injective, and we may conclude that W is itself a domain.

As we saw above, for any nonzero $x \in R$, there is a positive $n \in \mathbb{Z}$ so that $nx = xp(x^2)x \in [x^2]$ for some nonzero $p(Y) \in \mathbb{Z}[Y]$. Since $n^\# - (xp(x^2))^\# \in W$ has x in its kernel, we must have

$$n^\# = (xp(x^2))^\# \in [x^\#].$$

Let T be any nonzero subring of W . If $T \subseteq \mathbb{Z}^\#$, then our computation shows that, for any nonzero $x \in R$, $S^\# = T \cap [x^\#] \neq (0)$: if $0 \neq k^\# \in T$ and $0 \neq n^\# \in [x^\#]$, then for $m = kn$, $m^\# \in S^\#$. Thus, $S^\# \subseteq R^\#$ is a subring of T and of $R^\#$, and for some positive integer m , $m^\# \in S^\#$. When, instead, $T \subseteq R^\#$, then certainly $T \cap \mathbb{Z}^\# \neq (0)$ as above, so some $m^\# \in T$ for $m > 0$. Finally, when T contains a nonzero element $z^\# + a^\#$ with $z^\# \neq 0$ and $a^\# \neq 0$, then for a positive integer k with $k^\# \in [a^\#]$,

$$\begin{aligned} k(z^\# + a^\#) &= kz^\# + ka^\# = k^\#z^\# + ka^\# = z^\#k^\# + ka^\# \\ &= zk^\# + ka^\# \in T \cap [a^\#] \neq (0), \end{aligned}$$

and again T contains a nonzero subring of $R^\#$, which also contains some $m^\#$ for some $m > 0$.

Thus, in all cases, any nonzero subring T of W contains a nonzero subring $S^\#$ of $R^\#$ that also contains some $n^\# \in \mathbb{Z}^\#$ with $n > 0$. Since $R^\# \cong R$, we may write

$$R^\# = \bigcup (S^\# + r_i^\#)$$

for a finite $\{r_j^\#\} \subseteq R^\#$. It follows that

$$W = \bigcup (S^\# + z^\# + r_i^\#)$$

for $0 \leq z < n$ and $r_i^\# \in \{r_j^\#\}$. Therefore, $[W : S^\#]$ is finite, and since $S^\# \subset T$ we also have $[W : T]$ is finite.

We proved above that a commutative ring with identity element for which each nonzero subring has finite index must be isomorphic to the ring \mathbb{Z} . Thus, $W \cong \mathbb{Z}$ and, since $R^\#$ is an ideal in W , we must conclude that, for some positive integer m ,

$$R \cong R^\# \cong m\mathbb{Z}$$

as rings, completing the proof of the theorem. \square

Our final comments concern the situation when every nonzero Lie ideal of an infinite ring R has finite index in $(R, +)$. Recall that a Lie ideal of R is any additive subgroup L so that, for all $x \in L$ and all $r \in R$,

$$xr - rx = [x, r] \in L.$$

From this definition, it is clear that in a commutative ring R any additive subgroup is a Lie ideal. Thus, if R is an infinite commutative ring in which every nonzero Lie ideal has finite index in R , then R is a standard example by Theorem 2. Consequently, the only interest in considering Lie ideals is for noncommutative rings. Now every ideal of R is a Lie ideal, so assuming the finite index condition for Lie ideals, we have by Theorem 1 that R is a prime ring or $R^2 = (0)$ and

$$(R, +) \cong \mathbb{Z}.$$

Using these observations, we can prove the following:

Theorem 5. *Let R be an infinite ring so that for every nonzero Lie ideal L the index $[R : L]$ of $(L, +)$ in $(R, +)$ is finite. Then $R^2 = (0)$ and $(R, +) \cong \mathbb{Z}$; as rings $R \cong m\mathbb{Z}$ for some $m \geq 1$; or R is a prime ring with center $Z(R) = (0)$. Further, if R is a simple ring, then either $L = R$ for all nonzero Lie ideals L , or the centroid F of R must be finite, so $\text{char } R = p > 0$, and R contains only finitely many Lie ideals.*

Proof. Since any ideal of R is a Lie ideal, Theorem 1 shows that R is a standard example or is a prime ring, so we may assume that R is prime. Assume that $Z(R) \neq (0)$, and note that $Z(R)$ is a Lie ideal of R . Thus, $R/Z(R)$ is a finite additive abelian group so there is a

positive integer m with $mR \subseteq Z(R)$, and there is $\{a_1, \dots, a_k\} \subseteq R$ with $R = \bigcup(Z(R) + a_j)$. It follows first that, for any $s, t \in R$,

$$[s, t] = [a_i, a_j]$$

for some $1 \leq i, j \leq k$, and then, using

$$m[a_i, a_j] = [ma_i, a_j] = 0,$$

that $[R, R]$ is finite. But $[R, R]$ is a Lie ideal of R , so either R is commutative and applying Theorem 2 finishes the proof, or $R/[R, R]$ is finite forcing R to be finite. Consequently, we may assume that $Z(R) = (0)$.

For the last statement of the theorem, when R is simple with centroid F and contains a nonzero proper Lie ideal L , we follow the argument in the proof of Theorem 3. Since $[L, R] \subseteq L$ and $Z(R) = (0)$, we have that $[L, R]$ is a proper nonzero Lie ideal of R . Using that

$$[L, R] = [L, FR] = F[L, R]$$

is also an F -vector space, we conclude that $R/[L, R]$ is finite, not zero and an F -vector space, so F must be finite.

Further, R a simple ring with $Z(R) = (0)$ implies that every nonzero Lie ideal of R must contain $[R, R]$ [4, page 9, Theorem 1.5]. Either $[R, R] = R$ or $[R, R]$ is the unique, minimal, nonzero Lie ideal in R . In this case, $R/[R, R]$ is finite, so there are only finitely many additive subgroups of R containing $[R, R]$. Hence, R can contain only finitely many Lie ideals. \square

It is not obvious that examples of noncommutative rings satisfying the hypothesis of Theorem 5 exist, and if so whether any can be simple. A prime ring that satisfies the conditions of Theorem 5 must be highly noncommutative, since any prime ring satisfying a polynomial identity has a nontrivial center [14]. In addition, most standard examples of infinite, noncommutative, prime rings contain Lie ideals of infinite index. We present some examples relevant for Theorem 5. Our first one is a simple algebra with finite centroid. We then can describe some finite extensions of it that are examples of prime rings that are not simple and satisfy the finite index condition of Theorem 5.

Example 2. As in Example 1, for K a finite field, let $M_0(K)$ be the ring of all countable by countable matrices over K with only finitely many nonzero entries. It is straightforward to show that $M_0(K)$ is a simple ring, that

$$[M_0(K), M_0(K)]$$

consists of all matrices in $M_0(K)$ having trace zero, and that

$$M_0(K)/[M_0(K), M_0(K)] \cong e_{11}K$$

as additive groups, for the usual matrix unit e_{11} . Since $M_0(K)$ is a simple ring with zero center, as above, every nonzero, proper Lie ideal of $M_0(K)$ contains

$$[M_0(K), M_0(K)]$$

[4, page 9, Theorem 1.5]. Thus, $M_0(K)$ is a simple ring with finite centroid K so that $M_0(K)/L$ is finite for every nonzero Lie ideal of $M_0(K)$.

Just as in Example 1, we can extend Example 2 to find some prime, but not simple rings, satisfying the finite index condition in Theorem 5.

Example 3. Let $S \subseteq M_n(K)$ for $n > 1$, and let K be a finite field, so that S is a subring containing no invertible matrix in $M_n(K)$. An example would be the subring of strictly upper triangular matrices, perhaps with arbitrary entries in a subset of positions on the main diagonal. As in Example 1, let R be the subring of the countable by countable matrices over K generated by $M_0(K)$ in Example 2, and, for some $n > 1$, the block diagonal $n \times n$ matrices with each diagonal block the same fixed element of S : these have $A \in S$ in the upper left corner, and A is repeated consecutively and infinitely down the diagonal. Then it is easy to see that R is a prime ring with unique, nonzero, minimal ideal $M_0(K)$.

If L is any nonzero Lie ideal of R , then since

$$Z(R) = (0),$$

$[L, L] \neq 0$ [12, page 120, Lemma 6], and it follows that L must contain $[M_0(K), M_0(K)]$ [12, page 123, Theorem 13]. As in Example 2, the cosets of $[M_0(K), M_0(K)]$ in $M_0(K)$ are generated by $e_{11}K$, so the

cosets of

$$[M_0(K), M_0(K)]$$

in R are generated by the elements of $e_{11}K \cup S$, a finite set. Thus, R/L must be finite. The choice of S containing no invertible matrix is essential for ensuring that R has no center.

Our final example is a simple ring, of any characteristic, that contains no proper, nonzero Lie ideal.

Example 4. A result of Harris [3] constructs division rings D , for each possible characteristic, that satisfies

$$[D, D] = D.$$

Further, for any $d \in D$, there are $a, b \in D$ so that

$$d = [a, b] = ab - ba.$$

Let $R = M_0(D)$ be as in Example 1; R is the ring of countable by countable matrices with entries in D so that each matrix has only finitely many nonzero entries. Since D is a simple ring, it follows easily that R is as well, and that $Z(R) = (0)$. As in Example 2, every nonzero Lie ideal of R contains $[R, R]$. Using that $[D, D] = D$, a direct computation with matrix units in R shows that $[R, R]$ contains

$$e_{ij}[D, D] = D_{ij} \quad \text{for all } i, j.$$

This means that

$$[R, R] = R,$$

so R is the only proper Lie ideal in R .

In the same way that Example 3 obtained prime rings via finite extensions of the simple ring in Example 2, one can obtain prime, finite extensions of the simple ring $M_0(D)$ in Example 4 when the division ring D has prime characteristic. In this case, the center of D contains finite subfields, say K is such. In analogy with Example 3, if, for any $n > 1$ $S \subseteq M_n(K)$ is a subring without an identity element, then define R to be the ring generated by $M_0(D)$ and the block diagonal matrices with a fixed entry $A \in S$ in each diagonal block.

The examples above for Theorem 5 are all of the following form: R is a prime ring with $Z(R) = (0)$ and is a finite extension of an ideal M so that M is a simple ring with unique, nonzero, minimal Lie ideal L , necessarily $[M, M]$ (see [4]), of finite index in R . Any such ring must satisfy the hypothesis of Theorem 5. For, if V is a nonzero Lie ideal of R , then by [12, page 120, Lemma 6], for some ideal I of R ,

$$[I, I] \subseteq V.$$

Since $M = MI \subseteq I$, we must have

$$[M, M] \subseteq V,$$

so $[M, M]$ is the unique, minimal Lie ideal in R (and in M), and $R/[M, M]$ finite forces R/V to be finite.

We have been unable to find examples for Theorem 5 of prime rings that are not simple and that are not of the form just mentioned above. Are there infinite, noncommutative rings that satisfy the assumption in Theorem 5 but do not contain a (unique) nonzero simple ideal? In any case, could there be a noncommutative ring containing an infinite collection of Lie ideals that satisfies the assumption in Theorem 5? We suspect that, if an infinite, noncommutative, prime ring R satisfies the finite index condition for its nonzero Lie ideals, then R must contain only finitely many Lie ideals, or at least must satisfy the descending chain condition on Lie ideals. In the latter case, R would contain a unique, minimal, nonzero Lie ideal, so only finitely many Lie ideals. We have been unable to prove such a result.

REFERENCES

1. Y. Fedorov, *On infinite groups of which all nontrivial subgroups have finite index*, Uspek. Mat. Nauk. **6** (1951), 187–189.
2. R. Gilmer, *A note on rings with only finitely many subrings*, Script. Math. **29** (1973), 37–38.
3. B. Harris, *Commutators in division rings*, Proc. Amer. Math. Soc. **9** (1958), 628–630.
4. I.N. Herstein, *Topics in ring theory*, University of Chicago Press, Chicago, 1969.
5. Y. Hirano, *Some finiteness conditions for rings*, Chinese J. Math. **16** (1988), 55–59.

6. A.A. Klein, *The finiteness of a ring with a finite maximal subring*, Comm. Alg. **21** (1993), 1389–1392.
7. K. Koh, *On properties of rings with a finite number of zero divisors*, Math. Ann. **171** (1967), 79–80.
8. T.J. Laffey, *A finiteness theorem for rings*, Proc. Roy. Irish Acad. **92** (1992), 285–288.
9. C. Lanski, *Rings with few nilpotents*, Houston J. Math. **18** (1992), 577–590.
10. ———, *Higher commutators, ideals and cardinality*, Bull. Austr. Math. Soc. **54** (1996), 41–54.
11. ———, *A characterization of infinite cyclic groups*, Math. Mag. **74** (2001), 61–65.
12. C. Lanski and S. Montgomery, *Lie structure of prime rings of characteristic 2*, Pac. J. Math. **42** (1972), 117–136.
13. J. Lewin, *Subrings of finite index in finitely generated rings*, J. Alg. **5** (1967), 84–88.
14. L. Rowen, *Some results on the center of a ring with polynomial identity*, Bull. Amer. Math. Soc. **79** (1973), 219–223.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF SOUTHERN CALIFORNIA, 3620
SOUTH VERMONT AVENUE, LOS ANGELES CA 90089

Email address: clanski@usc.edu