COMMUTATIVE RINGS WITH HOMOMORPHIC POWER FUNCTIONS

DAVID E. DOBBS

Department of Mathematics
University of Tennessee
Knoxville, TN 37996–1300

JOHN O. KILTINEN

Department of Mathematics & Comp. Sci.
Northern Michigan University
Marquette, MI 49855–5340

BOBBY J. ORNDORFF

Department of Mathematics
Virginia Polytechnic Institute and State University
Blacksburg, VA 24061–0106

(Received July 25, 1990 and in revised form August 15, 1991)

ABSTRACT. A (commutative) ring R (with identity) is called *m–linear* (for an integer $m \geq 2$) if $(a + b)^m = a^m + b^m$ for all a and b in R. The m–linear reduced rings are characterized, with special attention to the finite case. A structure theorem reduces the study of m–linearity to the case of prime characteristic, for which the following result establishes an analogy with finite fields. For each prime p and integer $m \geq 2$ which is not a power of p, there exists an integer $s \geq m$ such that, for each ring R of characteristic p, R is m–linear if and only if $r^m = r^{p^s}$ for each r in R. Additional results and examples are given.

KEY WORDS AND PHRASES. Commutative ring, m–linear, characteristic, direct product, field, Jacobson radical, reduced ring.

1991 AMS SUBJECT CLASSIFICATION CODES. Primary 13A99; Secondary 12E99; 13G05; 13A10.

1. INTRODUCTION.

Let R be a ring and $m \geq 2$ an integer. (Except in Remark 7.4, rings are assumed to be commutative, with identity.) Following [1], we say that R is *m–linear* in case $(a + b)^m = a^m + b^m$ for all a and b in R; that is, in case the power function $r \mapsto r^m$ is a ring endomorphism of R. (In [2], m–linear domains and fields were studied under the terminology of m–domains and m–fields. The references in [1] cite other algebraic contexts where endomorphic power functions have been studied.) The simplest examples of m-linear rings are the rings of prime characteristic p in case m is a power of p: see the easy proofs involving binomial coefficients in [1] and [2]. In [1, Theorem 5] and [2, Theorem 2.3], it is shown that this relationship between characteristic and exponent is necessary in a number of cases of m–linearity. However, "exceptional" instances of m–linearity abound: consider the table in [2, page 52] and the examples in [2, Theorem 3.1]. The main results of this paper explain this diverse behavior.

The explanation is two-fold. First, via standard methods, Theorem 2.2 reduces the study of m-linear rings to the case of prime characteristic p. Within this case, the above comments permit us to focus on the subcase in which m is not a power of p. For m and p as in this subcase, m-linearity is explained in this paper's main result, Theorem 6.4: there exists an integer $s \geq m$ such that a ring R of characteristic p is m-linear if and only if $r^m = r^{p^s}$ for each r in R. In other words, for this subcase, m-linearity just amounts to the simple paradigm of p^s-linearity.

Theorem 6.4 depends on a number-theoretic result (see Proposition 6.2) and on much of the preceding material in this paper. Relevant results (for the subcase of prime p and m not a power of p) include a bound on indices of nilpotence in an m-linear ring (Theorem 4.3(a)) and an additive decomposition involving a canonical reduced subring of an m-linear ring (Theorem 4.5). In part for this reason, reduced m-linear rings are studied closely (Theorem 4.1, Corollary 4.2), especially in the finite case (Theorem 5.3). This work builds on an effective characterization of the m-linear fields in Theorem 3.1, which answers a question left open in [2].

If R is a ring, J(R) denotes the Jacobson radical of R, N(R) denotes the prime radical (set of nilpotent elements) of R, and $R_{red} = R/N(R)$ denotes the associated reduced ring of R. As usual, F_q denotes the finite field of cardinality q. Apart from some familiarity with [2] and [1], we assume only elementary number theory and standard abstract algebra, as in [3].

2. A STRUCTURE THEOREM.

In this section, we collect some useful facts and then give a result that reduces the study of m-linearity to the case of prime characteristic.

LEMMA 2.1.

(a) *If R is m-linear, then $n = char(R)$ is nonzero and the following two equivalent conditions hold:*

(i) *$k^m \equiv k \pmod{n}$ for each positive integer k;*

(ii) *n is square-free and $m \equiv 1 \pmod{p-1}$ for each prime divisor p of n.*

(b) *Let $R = \Pi R_i$ be the direct product of a family of rings R_i. Then R is m-linear if and only if R_i is m-linear for each index i.*

(c) *Subrings and homomorphic images of m-linear rings are also m linear.*

(d) *If R is m-linear, then so is R_{red}.*

PROOF. (a) The fact that $n \neq 0$ was observed in [2, page 53] as a consequence of the fact that R cannot contain a copy of Z. The other assertions in (a) are from [1, Lemmas 1 and 2, Theorem 1].

(b) This is a restatement of [1, Lemma 3(a)], included here for reference purposes.

(c) The first assertion is obvious. For the second, consider a ring-homomorphism $f: R \rightarrow S$ where R is m-linear; write $s_i = f(r_i)$ with $s_i \in S$ and $r_i \in R$; and notice that applying f to the equation $(r_1 + r_2)^m = r_1{}^m + r_2{}^m$ leads to $(s_1 + s_2)^m = s_1{}^m + s_2{}^m$. (Notice that the second assertion also gives a new proof of the "only if" assertion in (b).)

(d) This follows directly from the second assertion in (c) since $R_{red} = R/N(R)$ is a homomorphic image of R. ∎

THEOREM 2.2. *Let* R *be a ring and* $n = char(R)$. *Then* R *is m–linear if and only if* $n = p_1 \dots p_k$ *for some pairwise distinct primes* $p_1, \dots, p_k$ *and* $R = \Pi R_i$ *where, for each* i, R_i *is an m–linear ring of characteristic* p_i.

PROOF. The "if" assertion follows directly from Lemma 2.1(b). For the converse, assume that R is m–linear. By Lemma 2.1(a), $n = p_1 \cdot \dots \cdot p_k$ for some pairwise distinct primes p_i. As a torsion abelian group, R is the direct sum of its p_i–primary subgroups (cf. [3, hint for Exercise 7, page 82]). In other words, $R = \oplus R_i$, where $R_i = \{ r \in R \mid p_i \cdot r = 0 \}$. Write $1 = \Sigma e_i$, with $e_i \in R_i$. Hence $x = \Sigma x e_i$ for each x in R. It is clear that R_i is a ring. To show that e_i is its identity element and that R is a ring direct sum of the R_j's, it suffices to prove $R_i R_j = \{ 0 \}$ whenever $i \neq j$. However this is clear since $Ann_Z(R_i R_j) \supset Ann_Z(R_i) + Ann_Z(R_j) = p_i Z + p_j Z = Z$. Moreover, char $(R_i) = p_i$ by the definition of R_i; and R_i is m–linear by Lemma 2.1(b)(or (c)). ▮

The reader may have noticed that the proof of Theorem 2.2 leads to a decomposition for any n–torsion ring when n is square–free; the case addressed in Theorem 2.2 is tailored to fit our needs in §6. Although our main interest in Theorem 2.2 is its focus on rings of prime characteristic, we close the section with a simple consequence that leads naturally to the topics of §§3, 4, while also giving a partial converse of Lemma 2.1(a).

COROLLARY 2.3. *Let* m *and* n *be integers each greater than or equal to* 2. *Then the following three conditions are equivalent:*

(1) n *is square–free and* $m \equiv 1 \pmod{p-1}$ *for each prime divisor* p *of* n;

(2) $n = p_1 \dots p_k$ *for pairwise distinct primes* p_i *and, for each* i, *the finite field* Fp_i *is m–linear;*

(3) Z/nZ *is m–linear.*

Moreover, the above conditions imply, but are not implied by,

(4) Z/nZ *is reduced.*

PROOF. (4) is equivalent to the condition that n is square–free. Hence, (1) ⇒ (4). However, it is easy to see that (4) ⇏ (1): consider, for instance, $m = 2, n = 3 = p$.

It is shown in [1, Theorem 2] that (1) ⇔ (3). It is possible to'extract the implication (3) ⇒ (2) from the proof of Theorem 2.2. However, matters are really simpler. Given *either* (2) or (3), we have $n = p_1 \cdot \dots \cdot p_k$ for distinct primes p_i (invoking Lemma 2.1(a) in case (3) is given), and so $Z/nZ \cong \Pi Fp_i$ by the Chinese Remainder Theorem. An application of Lemma 2.1(b) now yields (3) ⇔ (2). ▮

A slightly different proof of Corollary 2.3 would be available in the next section, for the above appeal to [1, Theorem 2] could be replaced by citing Theorem 3.1.

3. m–LINEAR DOMAINS.

In this section, we answer some questions that were left open in [2] concerning m–linear domains and m–linear fields.

THEOREM 3.1. *Let* $m \geq 2$ *be an integer and* $q = p^k$ *be a power of a prime* p. *Then the following conditions are equivalent:*

(1) $m \equiv p^i \pmod{q-1}$ *for some* $i = 1, 2, \dots, k$;

(2) There exists i, $1 \le i \le k$, such that $r^m = r^{p^i}$ for each r in F_q;

(3) F_q is m–linear.

PROOF. (3) ⇒ (2): Let $\sigma: F_q \to F_q$ be the Frobenius map; that is, $\sigma(r) = r^p$. By Galois theory, $\mathrm{Gal}(F_q/F_p) = \langle\sigma\rangle = \{ \sigma^i \mid 1 \le i \le k \}$. Assume (3). Define $\tau: F_q \to F_q$ by $\tau(r) = r^m$. Since τ is a (nontrivial) ring–homomorphism of fields, τ is injective and so, by the pigeonhole principle, τ is surjective; that is $\tau \in \mathrm{Gal}(F_q/F_p)$. Hence $\tau = \sigma^i$, with $1 \le i \le k$. Thus $r^m = \tau(r) = \sigma^i(r) = r^{p^i}$ for each r in F_q.

(2) ⇒ (1): Assume (2). Let r be a generator of the (cyclic) multiplicative group of F_q. The order of r is $|F_q \setminus \{0\}| = q-1$. But (2) yields $r^m = r^{p^i}$, whence $r^{m-p^i} = 1$. Hence $m-p^i$ is divisible by the order of r; that is, (1) holds.

(1) ⇒ (3): Assume (1). Write $m = p^i + d(q-1)$ for some integer d. If $r \in F_q \setminus \{0\}$, then $r^{q-1} = 1$, and so $r^m = r^{p^i}(r^{q-1})^d = r^{p^i} \cdot 1 = r^{p^i}$. Of course, $r = 0$ also satisfies $r^m = r^{p^i}$ Hence (2) holds. Since F_q is p^i–linear (cf. [1, Lemma 4] or [2, Proposition 2.1(d)]), $(r_1 + r_2)^{p^i} = r_1^{p^i} + r_2^{p^i}$ for each r_1, r_2 in F_q. It follows that $(r_1 + r_2)^m = r_1^m + r_2^m$; that is, (3) holds. ∎

Theorem 6.4 will produce a characterization of the m–linear rings of characteristic p that is motivated by condition (3) in Theorem 3.1. For the moment, we pause to illustrate Theorem 3.1 by finding all the 15–linear domains. By [2, Corollary 2.4], these are just F_2 and the so–called "15–exceptions," which are certain other F_q with $q < 15$. The only values of q between 3 and 14 which satisfy condition (1) in Theorem 3.1, with $m = 15$, are $q = 3$ and $q = 8$. Hence the only 15–linear domains are F_2, F_3 and F_8.

It is convenient next to recall the following material from [2, page 54]. If $m \ge 2$ is an integer, then an *m–exception* is an m–linear domain R such that R is not isomorphic to F_2 and m is not a power of char(R); any m–exception is necessarily a finite field of cardinality less than m. The next result relates to questions raised in [2, page 55]. It identifies a special role for F_3: cf. the role found for F_2 in [2, Corollary 2.6].

COROLLARY 3.2.

(a) F_3 is m–linear for each odd integer $m \ge 3$. (If, in addition, m is not a power of 3, then F_3 is an m–exception.)

(b) Let $q \ge 4$ be a power of a prime. Then there exists an odd $m \ge 3$ such that F_q is not m–linear.

PROOF. (a) By Theorem 3.1, F_p is m–linear if and only if $m \equiv p \pmod{p-1}$; that is, if and only if $m \equiv 1 \pmod{p-1}$. The assertion follows, with $p = 3$, since $m - 1$ is even.

(b) Write $q = p^k$ for some prime p and positive integer k. By Theorem 3.1, there are exactly k integers m between 2 and q such that F_q is m–linear (namely, $m = p, p^2, \ldots, p^k = q$). The number of odd integers $m \ge 3$ between 2 and q is $q/2 - 1$ or $(q-1)/2$ according as to whether p is 2 or odd.

Suppose $p = 2$. In this case, it suffices to show that $k < 2^{k-1} - 1$ $(= q/2 - 1)$. This can easily be established by induction if $k \ge 4$. So, it remains to show that F_4 and F_8 are not m-linear for some odd m. In fact, $m = 3$ works: see the table in [2, page 52] or appeal to [4, Exercise 6(c), page 10] or notice that condition (1) in Theorem 3.1 is not satisfied.

The argument for odd p is similar. If $p = 3$ (and so $k \ge 2$), we have easily by induction that $k < (3^k - 1)/2$ or equivalently, $2k < 3^k - 1$. For $p \ge 5$, we verify that $k < (p^k - 1)/2$

or equivalently, $2k < p^k - 1$, as follows. For $k = 1$, the assertion holds since $3 < p$; and for $k \geq 2$, just notice that $2k < 3^k - 1 < p^k - 1$. ▮

The final result in this section is interesting in part because its statement does not mention m–linearity. Its proof touches on a concept developed further in §7.

COROLLARY 3.3. *Let $m \geq 2$ be an integer and $q = p^k$ be a power of a prime p. Put $f = X^q - X$ and $g = (X + 1)^m - X^m - 1$ in $F_p[X]$. Then $f | g$ in $F_p[X]$ if and only if $m \equiv p^i$ (mod $q - 1$) for some $i = 1, 2, ..., k$.*

PROOF. It is well known that f has q distinct roots, namely the elements of $\mathbf{F}_q$. Thus $f | g$ if and only if $g(r) = 0$ for each r in $\mathbf{F}_q$; that is, if and only if $(r + 1)^m = r^m + 1$ for each r in $\mathbf{F}_q$. By [2, Proposition 2.1(b)], this last condition is equivalent to $\mathbf{F}_q$ being m-linear. An appeal to Theorem 3.1 [(3) $\Leftrightarrow$ (1)] yields the asserted equivalence. ▮

4. m–LINEAR REDUCED RINGS.

According to [2, Corollary 2.4], the m–linear domains consist of $\mathbf{F}_2$; the domains of characteristic p, in case m is a power of p; and certain m–exceptions $\mathbf{F}_q$, with $q \leq m$, which can be effectively determined using condition (1) in Theorem 3.1. As we show in Theorem 4.1, this information leads to a characterization of the larger class of m–linear reduced rings. The ensuing focus on nilpotent elements leads eventually to a useful decomposition (in Theorem 4.5) that characterizes m–linearity in the important case of prime characteristic p, with m not a power of p.

THEOREM 4.1. *Let $m \geq 2$ be an integer and R a ring. Then the following conditions are equivalent:*

(1) R is reduced and $(r + 1)^m = r^m + 1$ for each r in R;

(2) R is (isomorphic to) a subring of a direct product of m–linear domains;

(3) R is reduced and m–linear.

PROOF. (2) $\Rightarrow$ (3): Suppose $R \subset \Pi D_i$, where each D_i is an m–linear domain. By Lemma 2.1(b) and (c), R is m–linear. Moreover, R is reduced since $N(R) \subset \Pi N(D_i) = \Pi\{0\} = \{0\}$.

(3) $\Rightarrow$ (1): Trivial.

(1) $\Rightarrow$ (2): Assume (1). Put $T = \Pi R/P$, where P ranges over the set of prime ideals of R. The kernel of the canonical ring–homomorphism $R \to T$ is $\cap P = N(R) = \{0\}$, since R is reduced, and so R can be identified with a subring of T. It remains to show, for each P, that the domain R/P is m–linear. We see, as in the proof of Lemma 2.1(c), that R/P inherits from R the property "$(a + 1)^m = a^m + 1$ for all a." Hence, by an appeal to [2, page 54], we have that R/P is m–linear, as desired. ▮

The next result sharpens condition (2) of Theorem 4.1 for certain cases.

COROLLARY 4.2. *Let R be a reduced m–linear ring of prime characteristic p, such that m is not a power of p. Then:*

(a) R is (isomorphic to) a subring of a direct product of m–linear finite fields of characteristic p.

(b) *Suppose, in addition, that R is finitely generated as an abelian group. Then $R = K_1 \times \dots \times K_t$, where each of the finitely many K_i is an m-linear finite field.*

PROOF. (a) View R as a subring of $\Pi R/P$, as in the proof that (1) ⇒ (2) in Theorem 4.1. Each R/P is an m-linear domain of characteristic p; since m is not a power of p, [2, Corollary 2.4] assures that R/P is a finite field (of cardinality less than m).

(b) Consider the positive square-free integer $p = \mathrm{char}(R)$. Now, R is a finitely generated (p-torsion) abelian group, hence finite. In particular, R is an artinian ring, and so each of the (finitely many) prime ideals P of R is maximal. By the Chinese Remainder Theorem, $R/\cap P \cong \Pi R/P$. By the proof of (a), each R/P is an m-linear finite field. Moreover, $R \cong R/\cap P$, since $\cap P = N(R) = \{ 0 \}$, completing the proof. (An alternate proof is available, using Wedderburn structure theory, picking up at the point where we noticed that R is finite, hence artinian. Let $J(R)$ be the Jacobson radical of R. Then the semisimple ring $R/J(R)$ is (isomorphic to) a product of (necessarily m-linear finite) fields. But $J(R) = N(R)$ (= $\{ 0 \}$) since R is artinian, whence $R \cong R/J(R)$.) ▮

Corollary 2.3 shows that Z/nZ must be reduced if it is m-linear for some $m > 1$. In the same spirit, the next result gives a sufficient condition for an m-linear, prime characteristic ring to be reduced.

THEOREM 4.3. *Let R be an m-linear ring of prime characteristic p. Then:*

(a) *Suppose that m is not a power of p; that is, $m = p^t e$, where $p \nmid e$ and $e > 1$. Then $r^{p^t} = 0$ for each r in $N(R)$.*

(b) *If $p \nmid m$, then R is reduced.*

PROOF. (a) Since R is m-linear, $(1 + r)^m = 1 + r^m$; that is, $(1 + r)^{p^t e} = 1 + r^{p^t e}$. However $(1 + r)^{p^t} = 1 + r^{p^t}$: this is trivial if $t = 0$ and follows from the p^t-linearity of R if $t \geq 1$. Hence $(1 + r^{p^t})^e = 1 + r^{p^t e}$. Expanding the left-hand side by the binomial theorem and rearranging, we have

$$\sum_{i=1}^{e-1} \binom{e}{i} r^{i p^t} = 0. \tag{4.1}$$

The coefficient of r^{p^t} is $\binom{e}{1} = e$ which is invertible in F_p ($\subset R$) since $p \nmid e$. Hence we can solve for r^{p^t}. Without loss of generality, $e > 2$. As all the later terms have r^{2p^t} as a common factor, the result is $r^{p^t} = r^{2p^t} s_1$, for some $s_1 \in R$. Replacing r with r^2, we obtain an $s_2 \in R$ in the same way such that $r^{2p^t} = r^{4p^t} s_2$. By iterating the process, we get s_3, s_4, ... in R such that $r^{2^{n-1}p^t} = r^{2^n p^t} s_n$ for each n. This yields $r^{p^t} = s_1 s_2 \dots s_n \, r^{2^n p^t}$ for each n. By hypothesis, $r^d = 0$ for some positive integer d. Pick n so that $2^n p^t \geq d$ (for instance, take $n = [\log_2(d)] + 1$). Then $r^{2^n p^t} = r^{2^n p^t - d} r^d = 0$, so $r^{p^t} = s_1 s_2 \dots s_n \cdot 0 = 0$, as asserted.

(b) Since $p \nmid m$, $t = 0$ in the notation of (a). Then by (a), $r = r^{p^t} = 0$ for each r in N(R); that is, R is reduced. ▮

Remark 5.4 will illustrate Theorem 4.3(b). The next result builds on the proof of Theorem 4.3(a). It leads to Theorem 4.5, the promised decomposition that characterizes m-linearity in important cases.

PROPOSITION 4.4. *Let R be a reduced m-linear ring of prime characteristic p, such that m is not a power of p. Then $r \mapsto r^m$ is an automorphism of R.*

PROOF. Define $f: R \to R$ by $f(s) = s^m$ for each s in R. Since R is m-linear, f is a ring-homomorphism. Since R is reduced, $\ker(f) = \{0\}$; that is, f is an injection. Fix r in R. Now, f restricts to an injective endomorphism, say g, of $T = \mathbf{F}_p[r]$. It suffices to show that g is surjective. By the pigeonhole principle, it is enough to show that T is finite. But the displayed equation (4.1) in the proof of Theorem 4.3(a) does not depend on whether r is nilpotent, and thus reveals that r is algebraic (hence integral) over $\mathbf{F}_p$. Hence T is finitely generated over $\mathbf{F}_p$, hence finite. ∎

THEOREM 4.5. *Let $m \geq 2$ be an integer and let R be a ring of prime characteristic p such that m is not a power of p. Write $m = p^t e$, where $p \nmid e$ and $e > 1$. Then R is m-linear if and only if the following two conditions hold:*

(i) *There exists an m-linear ring B such that $R = B \oplus N(R)$, the additive group direct sum of B and $N(R)$.*

(ii) *$s^{p^t} = 0$ for each $s \in N(R)$.*

Moreover, if the above conditions hold, then B is uniquely determined.

PROOF. We consider the "if" assertion first. Assume (i) and (ii). If $b \in B$ and $x \in N(R)$, the p^t-linearity of R yields

$$(b + x)^m = (b + x)^{p^t e} = (b^{p^t} + x^{p^t})^e = (b^{p^t} + 0)^e = b^{p^t e} = b^m \tag{4.2}$$

Hence, given $b_1, b_2 \in B$ and $x_1, x_2 \in N$, we have, with $r_i = b_i + x_i$, that

$$(r_1 + r_2)^m = ((b_1 + b_2) + (x_1 + x_2))^m = (b_1 + b_2)^m = b_1{}^m + b_2{}^m = r_1{}^m + r_2{}^m. \tag{4.3}$$

Thus R is m-linear.

Conversely, suppose that R is m-linear. Then (ii) follows from Theorem 4.3(a). Put $B = \{r^m \mid r \in R\}$. Since R is m-linear, B is a subring of R; and B is m-linear, by Lemma 2.1(c). If $b = r^m \in B \cap N(R)$, then $r \in N(R)$ (since $N(R)$ is a radical ideal), and so $r^{p^t} = 0$ by (ii), whence $b = r^{m-p^t} \cdot r^{p^t} = r^{m-p^t} \cdot 0 = 0$. Hence $B \cap N(R) = \{0\}$. It remains to show that $R = B + N(R)$. Consider s in R; put $d = s^m \in B$. Note that B is reduced since $B \cap N(R) = \{0\}$. Hence, applying Proposition 4.4 to B, we find an element c in B such that $d = c^m$. Then $(s - c)^m = s^m - c^m = d - d = 0$; in particular, $s - c \in N(R)$. Thus $s = c + (s - c) \in B + N(R)$, proving (ii).

Finally, we prove the uniqueness of B in (ii), assuming that R is m-linear. Suppose also that $R = D \oplus N(R)$, for some m-linear subring D of R. Since $x^m = x^{m-p^t} \cdot x^{p^t} = x^{m-p^t} \cdot 0 = 0$ for each x in $N(R)$, we have

$$B = \{r^m \mid r \in R\} = \{u^m + v^m \mid u \in D, v \in N(R)\} = \{u^m \mid u \in D\} = D; \tag{4.4}$$

the last equation follows by applying Proposition 4.4 to D. ∎

It is interesting to note, in the context of Theorem 4.5, that B and $R/N(R) = R_{\text{red}}$ are isomorphic as abelian groups.

Recall from Lemma 2.1(d) that if R is m-linear, then so is R_{red}. The converse is false; our next result presents the minimal counterexample.

EXAMPLE 4.6. Let R be the ring of dual numbers over F_2; that is, $R = F_2 [X]/(X^2) = \{ a + bx \mid a, b \in F_2 \}$, where $x = X + (X^2)$ in R satisfies $x^2 = 0$. Of course, R is a nonreduced 2-linear ring with exactly 4 elements. Note that R is not 3–linear : $(x + 1)^3 = x^3 + 3x^2 + 3x + 1 = 0 + 0 + x + 1 \neq 0 + 1 = x^3 + 1$. However, $R_{\text{red}} = R/N(R) = R/\{ 0, x \} \cong F_2$ *is* 3–linear.

This example raises the question of characterizing the 3–linear rings. Proposition 5.6 will produce such a characterization.

5. FINITENESS QUESTIONS.

Theorem 5.3 presents a characterization of the finite m–linear reduced rings. To prepare for this, we study a class of (necessarily commutative) rings. Proposition 5.1 admits an easy proof which is omitted. Example 5.2 is included as motivation and as a lemma for Theorem 5.3.

PROPOSITION 5.1. *Let $n \geq 2$ be an integer and R a ring such that $r^n = r$ for each r in R. Then R is reduced and n–linear.*

EXAMPLE 5.2. (a) Let $K_1, \ldots, K_t$ be finitely many finite fields, $t > 1$, with $|K_i| = q_i$. Put $R = K_1 \times \ldots \times K_t$ and $n = \Pi (q_i - 1) + 1$. Then R is a finite reduced n–linear nondomain and $r^n = r$ for each r in R.

Evidently, R is not a domain since $t > 1$. In view of Proposition 5.1, it suffices to show $r^n = r$ for each r in R. For this, it is enough to prove $x^n = x$ for each x in K_j. Without loss of generality, $x \neq 0$. Hence $x^{q_j - 1} = 1$. Raising this equation to the power $\Pi_{i \neq j} (q_i - 1)$, we have $x^d = 1$, where $d = \Pi (q_i - 1)$, and so $x^n = x^d x = x$, as desired.

(b) Let R be the ring considered in Example 4.6. Then R is a finite nonreduced 2-linear ring; and no integer $n \geq 2$ satisfies $r^n = r$ for each r in R.

THEOREM 5.3. *If R is a finite ring, then the following are equivalent:*

(1) There exists an integer $n \geq 2$ such that $r^n = r$ for each r in R;

(2) R is reduced and m–linear for some integer $m \geq 2$.

PROOF. (1) $\Rightarrow$ (2) by Proposition 5.1. Conversely, assume (2). As in the proof of Theorem 4.1, R is (isomorphic to) a subring of $\Pi R/P$, where P ranges over the prime ideals of R. Each of the (finitely many) R/P is a finite domain, hence a field. If R has a unique prime ideal, then R is a finite field and $r^m = r$ for each r in R, where $m = |R|$. If R has more than one prime ideal, then Example 5.2(a) produces a suitable n. ▮

REMARK 5.4. Consider the ring R in Example 5.2(a), in case $t = 2$ and $K_1 = K_2 = F_3$. Then $R = F_3 \times F_3$ is an m –linear ring, where $m = \Pi (q_i - 1) + 1 = 2 \cdot 2 + 1 = 5$; and R has characteristic $p = 3$. Since $p \nmid m$, R is the type of reduced ring studied in Theorem 4.3(b) (and more interesting than the illustrations afforded by the fields or domains in §§ 2, 3).

One should note that the construction in Example 5.2 does not always lead to $p \nmid m$: consider, for instance, $F_2 \times F_2$.

Theorem 5.3 established the converse of a weakened version of Proposition 5.1 for finite rings. This is best–possible: indeed, Example 5.5 shows that conditions (1) and (2) in Theorem 5.3 are not equivalent if R is infinite.

EXAMPLE 5.5. There exists an infinite reduced 3–linear ring R such that there is no integer $n \geq 2$ satisfying $r^n = r$ for each r in R. For the construction, take

$$R = \prod_{d=1}^{\infty} F_{3^d} = F_3 \times F_9 \times F_{27} \times \dots . \tag{5.1}$$

Of course, R is infinite and reduced; moreover, R is 3–linear since char(R) = 3. Now, consider $n \geq 2$. Pick d so that $n < 3^d$. Let x generate the (cyclic) multiplicative group $F_{3^d} \setminus \{ 0 \}$. Then the order of x is $3^d - 1$, which exceeds $n - 1$, and so $x^{n-1} \neq 1$. Thus $r = (1, \dots, 1, x, 1, \dots)$ satisfies $r^n \neq r$.

Examples 4.6 and 5.5 suggest the question of characterizing the 3–linear rings. Proposition 5.6 answers this question. In passing, we observe that a nonzero ring R is 2-linear if and only if char(R) = 2.

PROPOSITION 5.6. *A ring R is 3–linear if and only if $R \cong A \times B$, where A is a subring (possibly $\{ 0 \}$) of a product of copies of F_2 and B is either $\{ 0 \}$ or a ring of characteristic 3.*

PROOF. F_2, $\{ 0 \}$ and any ring of characteristic 3 are each 3–linear. Hence, by Lemma 2.1(b) and (c), any $A \times B$ as in the statements is 3–linear.

Conversely, suppose R is 3–linear. Hence $(1 + 1)^3 = 1^3 + 1^3$ in R; that is, $6 = 0$ in R. It follows that R is an algebra over $Z/6Z \cong F_2 \times F_3$. Thus $R \cong A \times B$, where A is an F_2-algebra and B is an F_3–algebra. If $B \neq \{ 0 \}$, then char(B) = 3. Similarly, either $A = \{ 0 \}$ or char(A) = 2. It remains only to show that if $A \neq \{ 0 \}$, then A embeds in a product of copies of F_2.

By Lemma 2.1(c), A is a 3–linear ring (of characteristic 2). Each a in A satisfies $(a + 1)^3 = a^3 + 1$, whence $a^2 + a = 0$, whence $a^2 = a$. By Proposition 5.1, A is reduced. Hence A embeds in $\prod A/P$, where P ranges over the prime ideals of A. It suffices to show that each such A/P is isomorphic to F_2. Since A/P is a 3–linear domain of characteristic 2, this holds: see [2, page 52] or [4, Exercise 6(c), page 10]. ∎

We close this section with some applications of Proposition 5.6.

REMARKS 5.7. (a) Because of Proposition 5.6, one can see that all 3–linear rings are rather uncomplicated. For one such example, consider the ring

$$F_3 [X]/(X^5) \times \{ (a,b,b,a,a,b,b,a,\dots) \in F_2 \times F_2 \times \dots \}. \tag{5.2}$$

(b) In Example 4.6, we saw that $R = F_2 [X]/(X^2) = F_2 [x]$ is not 3–linear. Proposition 5.6 provides another proof. Indeed, it suffices to verify that R cannot be embedded in $D = \prod F_2$; this holds since D is reduced and R isn't.

6. AN ANALOGY WITH FINITE FIELDS.

In view of Theorem 2.2, an "explanation" for the phenomenon of m–linearity hinges on the case of prime characteristic. Theorem 6.4 provides such an explanation, in the spirit of condition (2) in Theorem 3.1. The section begins with some preparatory number theory. Lemma 6.1 is given for reference purposes; its well known proof is omitted.

LEMMA 6.1. *Let p, a and b be positive integers, with $p \geq 2$. Then $p^a - 1 \mid p^b - 1$ if and only if $a \mid b$.*

The next result establishes a "universal" p–th power dependent upon m, not a power of p, that explains any m–linearity that occurs among fields of characteristic p.

PROPOSITION 6.2. *Let p be a prime and let m be an integer at least 2 that is not a power of p. Then:*

(a) Let $(i_1, k_1), \ldots, (i_n, k_n)$ be the list of all (i,k) such that $1 \leq i \leq k$ and $m \equiv p^i \pmod{p^k - 1}$; assume this list is nonempty. Then there is an integer s such that $s \equiv i_j \pmod{k_j}$ for $j = 1, \ldots, n$. Also, one may have $s \geq m$.

(b) There is an integer $s \geq m$ such that, for any finite field F of characteristic p, F is m–linear if and only if $r^m = r^{p^s}$ for each r in F.

PROOF. (a) First, we show that the list of (i, k)'s is finite, namely that k is bounded above (by $\log_p m$). Indeed, by Theorem 3.1, $F = F_{p^k}$ is m–linear if (i, k) is in the list. Since m is not a power of p, F is then either F_2 or an m–exception, whence Corollary 2.4 of [2] yields $p^k \leq m$, as desired.

Consider two distinct entries in the list, say (i_1, k_1) and (i_2, k_2). Without loss of generality, $i_2 \geq i_1$. We claim that $d = (k_1, k_2)$ divides $i_2 - i_1$. To see this, note first via Lemma 6.1 that

$$(p^d - 1) \mid (p^{k_j} - 1) \text{ and } (p^{k_j} - 1) \mid (m - p^{i_j}) \text{ for } j = 1 \text{ and } 2, \text{ and so} \tag{6.1}$$

$$(p^d - 1) \mid [(m - p^{i_1}) - (m - p^{i_2})] = p^{i_2} - p^{i_1} = p^{i_1}(p^{i_2 - i_1} - 1), \text{ whence} \tag{6.2}$$

$p^d - 1$ divides $p^{i_2 - i_1} - 1$. An application of Lemma 6.1 now yields the claim.

In view of the above claim, we may apply a well known variant of the Chinese Remainder Theorem, so as to produce an integer s satisfying the n congruences $s \equiv i_j \pmod{k_j}$. By adding a suitable multiple of $k_1 \cdot \ldots \cdot k_n$ to s, we can arrange that $s \geq m$.

(b) Keep the notation of (a); in particular, let $s \geq m$ be as in (a). By Theorem 3.1, (i, k) is in the above list if and only if F_{p^k} is m–linear and i is the unique integer, $1 \leq i \leq k$, such that $r^m = r^{p^i}$ for all r in F_{p^k}. If F is a finite field (indeed any ring) of characteristic p such that $r^m = r^{p^s}$ for each r in F, then we see as in the proof of Theorem 3.1 [(1) ⇒ (3)] that F is m–linear. (Thus, if the above list is empty, we may belatedly choose $s = m$; in this case, (b) holds vacuously.) It remains only to show that $r^m = r^{p^s}$ for each r in $F_j = F_{p^{k_j}}$, $j = 1, \ldots, n$. Since the multiplicative group $F_j \setminus \{0\}$ is cyclic, our task is to show $d_j = p^{k_j} - 1$ divides $m - p^s$ for $j = 1, \ldots, n$. Since d_j divides $m - p^{i_j}$ an equivalent task is to show $d_j \mid (m - p^{i_j}) - (m - p^s) = p^{i_j}(p^{s - i_j} - 1)$. It is equivalent to show that $d_j \mid p^{s - i_j} - 1$ or (equivalently by Lemma 6.1) that $k_j \mid s - i_j$, for $j = 1, \ldots, n$. This last condition is just a restatement of the congruences established in (a). ∎

REMARK 6.3. One cannot delete the hypothesis in Proposition 6.2 (and Theorem 6.4) that m is not a power of p. Indeed, if $r^p = r^{p^s}$ for all r in F_{p^k} for all $k \geq 1$, then $p^k - 1 \mid p^s - p$ for all k, a contradiction if $k \geq s$.

We now present this paper's main result.

THEOREM 6.4. *Let p be a prime and let $m \geq 2$ be an integer that is not a power of p. Then there exists an integer $s \geq m$ such that, for any ring R of characteristic p, R is m-linear if and only if $r^m = r^{p^s}$ for each r in R.*

PROOF. Take s as in Proposition 6.2. Then the "if" assertion follows easily, as in the proofs of Proposition 6.2 and Theorem 3.1.

Conversely, let R be an m–linear ring of characteristic p. By Theorem 4.5, write $R = B \oplus N(R)$ as an abelian group, where B is an m–linear subring of R. Note that B is reduced since $N(B) \subset B \cap N(R) = \{ 0 \}$. Write $m = p^t e$, with $p \nmid e$ and $e > 1$. Consider r in R; write $r = b + x$, with $b \in B$ and $x \in N(R)$. By Theorem 4.3, $x^{p^t} = 0$; since $p^t < m < p^s$, we also have $x^m = 0 = x^{p^s}$. Hence the m-linearity of R yields $r^m = b^m + x^m = b^m$; and similarly the p^s–linearity of R yields $r^{p^s} = b^{p^s}$. Thus, we may replace R with B; that is, assume R is reduced.

Since R is reduced, Corollary 4.2(a) permits us to view R as a subring of a product $T = \Pi F_i$ of some m–linear finite fields F_i of characteristic p. The condition "$r^m = r^{p^s}$" holds in each F_i by Proposition 6.2(b), hence it holds (componentwise) in T, and hence it holds in the subring R. ∎

7. MISCELLANEA.

In this final section, we explore two topics involving m–linearity. The first is the question whether a ring R is m-linear if (and only if) $(r + 1)^m = r^m + 1$ for each r in R. This question has an affirmative answer if R is a domain [2, page 54]; more generally, if R is reduced (see Theorem 4.1); and also if $R = Z/nZ$ (by an easy proof by induction that is left to the reader). Proposition 7.2 gives an affirmative answer in case R is quasilocal (that is, has a unique maximal ideal), but we must leave the general question open.

LEMMA 7.1. *Let R be a ring and m a positive integer. Then:*

(a) Let $u, v \in U(R)$, the set of invertible elements of R. Then $(r + u)^m = r^m + u^m$ for each r in R if and only if $(r + v)^m = r^m + v^m$ for each r in R.

(b) Suppose that $(r + 1)^m = r^m + 1$ for each r in R. Then $(r + j)^m = r^m + j^m$ for each r in R and j in $J(R)$.

PROOF. (a) It is enough to prove the "only if" assertion. For this, note that $(r + v)^m = [u^{-1}v(uv^{-1}r + u)]^m = (u^{-1}v)^m(uv^{-1}r + u)^m = (u^{-1}v)^m[(uv^{-1}r)^m + u^m] = (u^{-1}v)^m(uv^{-1}r)^m + (u^{-1}v)^m u^m = r^m + v^m$.

(b) Since $j + 1 \in U(R)$, it follows from (a) that $(r + j + 1)^m = r^m + (j + 1)^m$. The hypothesis permits this equation to be rewritten as $(r + j)^m + 1 = r^m + j^m + 1$, and so $(r + j)^m = r^m + j^m$. ∎

PROPOSITION 7.2. *Let R be a quasilocal ring and let $m \geq 2$ be an integer. Then R is m-linear if (and only if) $(r + 1)^m = r^m + 1$ for each r in R.*

PROOF. By Lemma 7.1, $(r + s)^m = r^m + s^m$ for each r in R and each s in $U(R) \cup J(R)$. This union is R since R is quasilocal, and so R is m-linear. ∎

REMARK 7.3. The above work raises the question of what is implied for a ring R if a given $i \in R\backslash U(R)$ and integer $m \geq 2$ satisfy $(r + i)^m = r^m + i^m$ for each r in R. An easy positive result is that $(r - i)^m = r^m + (-i)^m$ for each r in R. However, R need not be m-linear under these conditions. For instance, $(r + 2)^2 = r^2 + 2^2$ for each r in $\mathbf{Z}/4\mathbf{Z}$, although $\mathbf{Z}/4\mathbf{Z}$ is not 2–linear. Additional examples of this phenomenon are easy to find by taking $R = \mathbf{Z}/n\mathbf{Z}$, with $(i, m, n) = (2, 4, 8), (6, 4, 8)$ or $(3, 4, 6)$, for example.

The final topic in this section concerns the theory of m-linearity for arbitrary associative rings. Remark 7.4 summarizes some results in this regard which the second-named author will publish elsewhere.

REMARK 7.4. In this remark, we remove the hypotheses that rings be commutative and have an identity, and indicate some ways in which the ensuing theory of m-linearity differs from the earlier work in this paper. First, in contrast with Theorem 2.2, a ring of characteristic zero can be m-linear; consider the ring $X\mathbf{Z}[X]/(pX^m)$, where p is prime and m is a power of p. Second, the index of nilpotence corresponding to Theorem 4.3(a) becomes $m + p^t$, which is best-possible. Third, in the absence of commutativity, conditions (i) and (ii) in Theorem 4.5 do not imply m-linearity: consider the ring of upper triangular 2×2 matrices over a reduced m-linear ring (in the earlier sense) of prime characteristic. Fourth, examples show that the "only if" part of Theorem 6.4 does not carry over to the more general setting. Finally, not all m-linear rings can be embedded in m-linear rings with identity; criteria for such embeddability can be given.

REFERENCES

1. Kiltinen, J. O. Linearity of exponentiation, *Math. Mag. 52* (1979), 3–9.

2. Dobbs, D. E. Fields with the simple binomial theorem, *Math. Mag. 62* (1989), 52–57.

3. Hungerford, T. W. *Algebra,* Graduate Texts in Mathematics, vol. 73, Springer-Verlag, New York/Heidelberg/Berlin, 1974.

4. Dobbs, D. E. and Hanks, R. *A Modern Course on the Theory of Equations,* Polygonal Publ. House, Passaic, NJ, 1980.