A note on radical semisimple classes

By L. C. A. van Leeuwen (Groningen) and T. L. Jenkins (Laramie, Wyo.)

Section 1.

The purpose of this note is to investigate the character of those finite sets of finite fields which determine radical semisimple classes. These classes are provided with a lattice structure and properties of this lattice are found. Definitions of radical related terms can be found in [2] and for those of lattice related terms in [1]. As usual, *lcm* will mean the least common multiple, *gcd* the greatest common divisor, and $a|b$ means a divides b. *All rings considered will be associative.*

In [6], P. Stewart has completely characterized all radical semisimple classes as subdirect sums of strongly hereditary finite sets of finite field.

Definition 1. A class of rings C is called *strongly hereditary* if whenever $R \in C$ and S is a subring of R then $S \in C$.

Definition 2. Let K_n be the class of all rings R such that $x^n = x$ for every $x \in R$, $n = 2, 3, 4, \dots$.

Stewart also establishes in [6] that every ring in a given K_n is isomorphic to a subdirect sum of fields from a strongly hereditary finite set of finite fields. It is these sets of fields we investigate and the associated K_n.

Section 2.

Let Z_{p^n} be a finite field of order p^n, p a prime and n a positive integer. It is well known that the subrings of Z_{p^n} are exactly those fields of order p^m where $m|n$. Now consider the following finite set of finite fields:

$$S = \{Zp_1, Zp_1^2, \dots, Zp_1^{\alpha_1}, Zp_2, Zp_2^2, \dots, Zp_2^{\alpha_2}, \dots, Zp_n, Zp_n^2, \dots, Zp_n^{\alpha_n}\}$$

where the p_i are prime numbers, $i = 1, 2, \dots, n$. Although S satisfies the requirement to be strongly hereditary, there are more fields in S than will normally be needed in our context. Thus we make the following definition.

Definition 3. A set F will be called a *proper strongly hereditary* finite set of finite fields if whenever $Z_{p^n} \in F$ where n is the highest power of the prime p for which $Z_{p^n} \in F$, then $Z_{p^m} \in F$ only if $m|n$. Thus, for example, $\{Z_2, Z_3, Z_{3^3}\}$ is proper where as $\{Z_2, Z_{3^2}, Z_{3^3}\}$ is not.

For each radical semisimple class K_n of Definition 2 we want to find which strongly hereditary finite set of finite fields F_n determines K_n.

Lemma 1. *Let $R \in K_n$ and suppose M is a maximal ideal of R. Then R/M is a finite field and $|R/M|-1$ divides $n-1$, where $|R/M|$ denotes the order of R/M.*

Proof. R is von Neumann regular, since for $n=2$, $a^2=a$ for all $a \in R$ so $a=aaa$. For $n>2$, $a^n=a$ for all $a \in R$ so $a=aa^{n-2}a$. Hence R is Jacobson semisimple. Since R is commutative [3, p. 217], the Jacobson radical of R is the intersection of all maximal ideals of R. Hence R is isomorphic to a subdirect sum of fields [5, p. 119].

We note that R must have maximal ideals. For if R has no maximal ideals then R has no prime maximal ideals so R is β_s-semisimple, where β_s is the upper radical determined by all simple prime rings. But $\beta_s \subseteq G$, the Brown—McCoy radical and then, since R is commutative, $J(R)=G(R)$ [2, p. 118], a contradiction.

With R/M a field satisfying $x^n=x$ for every $x \in R/M$ we have that R/M must be a finite field. Now $R/M-\{0\}$ is a multiplicative (cyclic) group of finite order satisfying $x^{n-1}=1$ for every $x \in R/M-\{0\}$. Hence $|R/M|-1$ divides $n-1$, completing the proof.

Corollary 1. Let $R \in K_n$. Then R is a subdirect sum of a finite number of finite fields.

Proof. The finite number arises from the fact that there are only a finite number of possibilities for $|R/M|$ where M is a maximal ideal of R.

If R runs through all the distinct rings of K_n, then any prime power p^k with $p^k-1 \mid n-1$ is obtained as the order of a finite field Z_{p^k} such that $R/M \cong Z_{p^k}$ for some $R \in K_n$ and some maximal ideal M in R. This is clear, for let Z_{p^k} be a finite field with $p^k-1 \mid n-1$. For any $x \in Z_{p^k}$ one has $x^{p^k-1}=1$ implying $x^{p^k}=x$. Then if $n-1=q(p^k-1)$, $x^{n-1}=1$ and so $x^n=x$ for any $x \in Z_{p^k}$. Then $Z_{p^k} \in K_n$ with maximal ideal (0) so that $Z_{p^k}/(0) \cong Z_{p^k}$. Now define

$$F_n = \{Z_{p^k} : p^k-1 \text{ is a divisor of } n-1\}.$$

That is, F_n consists of all finite fields Z_{p^k} such that $|Z_{p^k}|-1$ divides $n-1$. We have then shown

Lemma 2. *A finite field $Z_{p^k} \in F_n$ if and only if $p^k-1 \mid n-1$.*

We note that $F_n \neq \varnothing$ since $|Z_2|-1=1 \mid n-1$ for any $n \geqq 2$. Determining which finite fields Z_{p^α} are in a given F_n is simply a matter of determining for which primes p does $p^\alpha-1 \mid n-1$ for some α. For example, $F_7=\{Z_2, Z_{2^2}, Z_3, Z_7\}$ because $2-1 \mid 6$, $2^2-1 \mid 6$, $3-1 \mid 6$, and $7-1 \mid 6$.

Lemma 3. *$R \in K_n$ if and only if R is a subdirect sum of fields from F_n.*

Proof. We have seen that if $R \in K_n$ then R is such a subdirect sum. Conversely, let R be a subdirect sum of fields from F_n. For $x \in R$ one has $x=(\dots, x_i, \dots)$ with entries $x_i \in Z_{p_i^{k_i}} \in F_n$. Then $p_i^{k_i}-1 \mid n-1$ so $x_i^{p_i^{k_i}-1}=1$ and hence $x_i^{n-1}=1$ and $x_i^n=x_i$ for all entries x_i in x. Hence $x^n=x$ for all $x \in R$ so $R \in K_n$.

Remark. It may be pointed out that for $n \neq m$, $F_n = F_m$ is possible and hence $K_n = K_m$. For example, $F_4 = \{Z_2, Z_2^2\} = F_{10}$.

As shown above, F_n can equal F_m with $n \neq m$. To obtain a well-defined lattice structure we must for any fixed positive integer $n \geqq 2$ consider all the $F_i = F_n$ and retain only that F_i with least index and omit all the others. This can be done in the following way. Let n be a fixed integer and suppose $\tau - 1 = lcm(p_i^{k_i} - 1)$ where $p_i^{k_i} - 1 \mid n - 1$. We show that $F_n = F_\tau$ and that τ is the least integer with the stated property. If $Z_{p_i^{k_i}} \in F_n$ then $x_i^{p_i^{k_i} - 1} = 1$ for any $x \in Z_{p_i^{k_i}}$ so $x^{\tau - 1} = 1$ and thus $x^\tau = x$ and $Z_{p_i^{k_i}} \in F_\tau$. On the other hand, suppose $Z_{p_i^{r_i}} \in F_\tau$. Then, by definition, $p_i^{r_i} - 1 \mid \tau - 1$ and $\tau - 1 \mid n - 1$ so for any $x \in Z_{p_i^{r_i}}$ we have $x^{\tau - 1} = 1$ and hence $x^{n-1} = 1$. It follows that $x^n = x$ and that $Z_{p_i^{r_i}} \in F_n$. Let $n \geqq 2$ be a fixed integer. We see that τ, with $\tau - 1 = lcm(p_i^{k_i} - 1)$, where $p_i^{k_i} - 1 \mid n - 1$, is the least integer for which $F_\tau = F_n$ by definition of least common multiple.

Henceforth then, we will assume when referring to any F_τ that $\tau - 1 = lcm(p_i^{k_i} - 1)$ where $p_i^{k_i} - 1 \mid \tau - 1$. We thus avoid any duplicity in the listing of the F_τ. To illustrate, we give the first few possible F_τ. With L denoting the entire set of F_τ we have

$$L = \{F_2, F_3, F_4, F_5, F_7, F_8, F_9, F_{11}, F_{13}, F_{15}, F_{16}, F_{17}, F_{19}, F_{21}, F_{22}, F_{23}, F_{25}, F_{27}, F_{29}, F_{31}, F_{32}, F_{37}, \ldots\}.$$

We note that $F_6 = F_{12} = F_{14} = F_{18} = F_{20} = F_{24} = F_{26} = F_{30} = \ldots = F_2$, $F_{10} = F_{28} = F_{34} = \ldots = F_4$, $F_{33} = \ldots = F_{17}$, $F_{35} = \ldots = F_3$, $F_{36} = \ldots = F_8$ and so forth.

Remark. The fields of a given K_n are exactly those in the corresponding F_n. We also note that the above results differ from those in [7, Chapter 6] and [8]. The following three points should also be made. First, not every strongly hereditary finite set of finite fields is exactly equal to some F_n. For example $\{Z_3, Z_{3^2}, Z_{3^3}\}$ is such a set, however it is a proper subset of $F_{105} = \{Z_2, Z_3, Z_{3^2}, Z_{3^3}, Z_5, Z_{53}\}$ and is not a subset of F_n for $n \leqq 104$. Secondly, every proper strongly hereditary finite set of finite fields is not necessarily some F_n for $\{Z_2, Z_{2^2}, Z_3\}$ is such a set and is not equal to any F_n and is a proper subset of F_{13}. Finally, while every F_n is necessarily a strongly hereditary finite set of finite fields, it need not be proper as is the case with $F_{22} = \{Z_2, Z_{2^2}, Z_{2^3}\}$.

Theorem 1. *The following are equivalent:*

1. $K_n \subseteqq K_m$.
2. $F_n \subseteqq F_m$.
3. *Whenever* $p^k - 1 \mid n - 1$, *then* $p^k - 1 \mid m - 1$.
4. $n - 1 \mid m - 1$.

PROOF. (1)→(2). Let $Z_{p^k} \in F_n$. Then $Z_{p^k} \in K_n \subseteqq K_m$ so $Z_{p^k} \in F_m$.
(2)→(3). Let $p^k - 1 \mid n - 1$. Then $Z_{p^k} \in F_n$ so $Z_{p^k} \in F_m$ and hence $p^k - 1 \mid m - 1$.

(3)→(4). We know that $n-1=lcm(p_i^{k_i}-1)$ where $p_i^{k_i}-1\,|\,n-1$. All such $p_i^{k_i}-1$ are divisors of $m-1$ and hence $lcm(p_i^{k_i}-1)\,|\,m-1$ so $n-1\,|\,m-1$. (4)→(1). Let $Z_{p^k}\in F_n$. Then $p^k-1\,|\,n-1$ so $p^k-1\,|\,m-1$. Hence $Z_{p^k}\in F_m$ and $F_n\subseteqq F_m$. If $R\in K_n$ then R is a subdirect sum of fields from F_n and hence of fields from F_m. Thus $R\in K_m$ and $K_n\subseteqq K_m$.

For integers n and m satisfying $n-1=lcm(p_i^{k_i}-1)$ where $p_i^{k_i}-1\,|\,n-1$ and $m-1=lcm(q_i^{\tau_i}-1)$ where $q_i^{\tau_i}-1\,|\,m-1$ we have F_n and F_m in L. These in turn determine radical semisimple classes K_n and K_m. Hence $K_n\cap K_m$ is a radical class and $K_n\cap K_m$ is a semisimple class [4]. Thus $K_n\cap K_m$ is a radical semisimple class and must equal some K_r.

Theorem 2. *If K_n and K_m are radical semisimple classes then $K_n\cap K_m=K_r$ is a radical semisimple class where $r-1=gcd(n-1, m-1)$.*

PROOF. We first show that $F_n\cap F_m=F_{r'}$ with $r'-1=gcd(n-1, m-1)$. Les $Z_{p^s}\in F_n\cap F_m (F_n\cap F_m\neq\emptyset$ for $Z_2\in F_n\cap F_m)$. Then $p^s-1\,|\,n-1$ and $p^s-1\,|\,m-1$ ot $p^s-1\,|\,gcd(n-1, m-1)=r'-1$. Thus $Z_{p^s}\in F_{r'}$. Conversely, if $Z_{p^u}\in F_{r'}$ then $p^u-1\,|\,r'-1$. But $r'-1\,|\,n-1$ and $r'-1\,|\,m-1$ so $p^u-1\,|\,n-1$ and $p^u-1\,|\,m-1$. It follows that $Z_{p^u}\in F_n\cap F_m$. Thus $F_n\cap F_m=F_{r'}$ where $r'-1=gcd(n-1, m-1)$. Now suppose $R\in K_{r'}$. Since $r'-1\,|\,n-1$, $K_{r'}\subseteqq K_n$ by the previous theorem and hence $R\in K_n$. Similarily $R\in K_m$ so $R\in K_n\cap K_m=K_r$. Thus $K_{r'}\subseteqq K_r$.

Conversely, if $R\in K_n\cap K_m=K_r$ then R is a subdirect sum of fields from F_r. A field in F_r is a field in K_r and hence both a field in K_n and K_m. Thus a field in F_r is a field in $F_n\cap F_m=F_{r'}$ or $F_r\subseteqq F_{r'}$ which implies $K_r\subseteqq K_{r'}$. Thus $K_r=K_{r'}$ and in particular $r=r'$ by our earlier identification. Hence $r-1=r'-1=gcd(n-1, m-1)$, completing the proof.

We see that the K_r of Theorem 2 will serve as the greatest lower bound for K_n and K_m. To obtain the second part of our lattice structure we now consider $F_n\cup F_m$. For $Z_{p^s}\in F_n\cup F_m$ either $Z_{p^s}\in F_n$ or $Z_{p^s}\in F_m$ or both. Hence $p^s-1\,|\,n-1$ or $p^s-1\,|\,m-1$ or both. Thus $p^s-1\,|\,lcm(n-1, m-1)$. Let $\tau-1=lcm(n-1, m-1)$. Then $n-1\,|\,\tau-1$, $m-1\,|\,\tau-1$ so $p^s-1\,|\,\tau-1$ and we have $Z_{p^s}\in F_\tau$. Hence $F_n\cup F_m\subseteqq F_\tau$ where $\tau-1=lcm(n-1, m-1)$. We must show with τ as defined that F_τ is the smallest F_k such that $F_n\subseteqq F_k$ and $F_m\subseteqq F_k$. Thus suppose $F_n\subseteqq F_k$ and $F_m\subseteqq F_k$. Then by Theorem 1 $n-1\,|\,k-1$ and $m-1\,|\,k-1$. Thus $\tau-1=lcm(n-1, m-1)\,|\,k-1$. Hence $F_\tau\subseteqq F_k$ and F_τ is the smallest such F_k.

From $F_n\subseteqq F_\tau$ and $F_m\subseteqq F_\tau$ if follows that $K_n\subseteqq K_\tau$ and $K_m\subseteqq K_\tau$. Now suppose $K_n\subseteqq K_s$ and $K_m\subseteqq K_s$. Then $F_n\subseteqq F_s$ and $F_m\subseteqq F_s$ so by the previous argument $F_\tau\subseteqq F_s$. Hence $K_\tau\subseteqq K_s$ and with $\tau-1=lcm(n-1, m-1)$ we have that K_τ is the smallest K_s such that $K_n\subseteqq K_s$ and $K_m\subseteqq K_s$.

Section 3.

With the notation of the previous section we now define:

$$K_n\vee K_m = K_\tau, \quad \tau-1 = lcm(n-1, m-1)$$

$$K_n\wedge K_m = K_r, \quad r-1 = gcd(n-1, m-1).$$

This enables us to make the collection of radical semisimple classes $\{K_n\}$, $n=2, \dots$, a lattice. This is clear, for the set $\{K_n\}$, $n=2, \dots$, is partially ordered by inclusion and the definitions of $\vee$ and $\wedge$ yield a *lub* and *glb* respectively for any two elements in the set.

Remark. K_τ, in general, is not the set theoretical union of K_n and K_m. For example, $K_3 \vee K_4 = K_7$ for $6 = lcm(2, 3)$. However, $Z_7 \in K_7$ but $Z_7 \notin K_3 \cup K_4$.

Now we consider some of the properties of this lattice. It is clear that the lattice is *not complete*, for an arbitrary collection of elements of the lattice does not have a least upper bound. It is also easy to see that the lattice is *not Brouwerian*. That is, for any two elements K_n and K_m there does not exist a largest K_s such that $K_n \wedge K_s \leqq K_m$.

Lemma 4. *The lattice of radical semisimple classes is distributive and so modular too.*

Proof. We must show [1, p. 39] that if $K_n \wedge K_m = K_n \wedge K_\tau$ and $K_n \vee K_m = K_n \vee K_\tau$ then $K_m = K_\tau$. That is, if $gcd(n-1, m-1) = gcd(n-1, \tau-1)$ and $lcm(n-1, m-1) = lcm(n-1, \tau-1)$ then $m=\tau$. By multiplying our assumptions we have

$$gcd(n-1, m-1)lcm(n-1, m-1) = gcd(n-1, \tau-1)lcm(n-1, \tau-1)$$

so that $(n-1)(m-1) = (n-1)(\tau-1)$. Hence $m-1 = \tau-1$ and $m=\tau$.

By definition, and in our notation, an *atom* of this lattice would be a K_n such that there does not exist a K_m where $K_2 \subsetneqq K_m \subsetneqq K_n$.

Lemma 5. *K_n is an atom in the lattice of radical semisimple classes if and only if $n=3$ or $n=2^\alpha$ where α is a prime number.*

Proof. From Theorem 1 we have $K_2 \subsetneqq K_m \subsetneqq K_n$ if and only if $F_2 \subsetneqq F_m \subsetneqq F_n$ and hence we can work with the F_n. It is clear that if F_n contains exactly two fields then F_n is an atom. Such is the case with $F_3 = \{Z_2, Z_3\}$. Every $F_n (\neq F_3)$ where n is odd necessarily contains F_3 properly and cannot be an atom. We need only to consider F_n where n is even. If $p^\alpha - 1 \mid n-1$ then $p^\alpha - 1$ must be odd and hence p^α must be even and so $p=2$. Thus the only fields in any F_n where n is even are of the form Z_{2^α} for some integer $\alpha \geqq 1$. Consider F_{2^β} where β is a prime number. If F_{2^β} was not an element in L then $F_{2^\beta} = F_\tau$ where $\tau - 1 = lcm(p_i^{\alpha_i} - 1)$ where $p_i^{\alpha_i} - 1 \mid 2^\beta - 1$.

Since F_{2^β} has an even subscript we have from the argument above that $p_i = 2$ for all i. Now $2^{\alpha_i} - 1 \mid 2^\beta - 1$ if and only if $\alpha_i \mid \beta$. But β is prime so $\alpha_i = 1$ or $\alpha_i = \beta$. Hence $\tau - 1 = lcm(2-1, 2^\beta - 1) = 2^\beta - 1$ and so $\tau = 2^\beta$ and $F_{2^\beta} \in L$. Also $F_{2^\beta} = \{Z_2, Z_{2^\beta}\}$ and hence is an atom. Suppose F_n, n even, contains a field of the form Z_{2^t} where t is not prime and let p be a prime divisor of t. Then, since F_n is strongly hereditary, $Z_{2^p} \in F_n$ and so $F_{2^p} = \{Z_2, Z_{2^p}\} \subsetneqq F_n$. Hence F_n cannot be an atom. Hence from Theorem 1 we have that the atoms are K_3 and K_{2^α} where α is prime.

Summarizing the above results we state

Theorem 3. *The set of radical semisimple classes $\{K_n\}$ $n=2, \dots$, determines a distributive lattice whose atoms are K_3 and K_{2^α} where α is prime.*

References

[1] G. Birkhoff, Lattice Theory, 3rd. ed., A.M.S., *Providence*, R. I., 1967.
[2] N. Divinsky, Rings and Radicals, Univ. of *Toronto* Press, 1965.
[3] N. Jacobson, Structure of Rings, A.M.S. Colloq, Pub. **37**, 1956.
[4] W. G. Leavitt, Sets of radical classes, *Publ. Math.* (Debrecen) **14** (1967), 321—324.
[5] N. Mc Coy, The Theory of Rings, *London*, 1964.
[6] P. Stewart, Semisimple radical classes, *Pac. J. Math.*, **32** (1970), 249—254.
[7] R. Wiegandt, Lectures on Radical and Semisimple Classes, Univ. of *Islamabad*, Pakistan, 1972.
[8] R. Wiegandt, Homomorphically closed semisimple classes, *Studia Univ. Babes—Bolyai*, Fasc. **17**/2. (1972), 17—20.

(Received July 1, 1973.)