SMARANDACHE-GALOIS FIELDS

W. B. Vasantha Kandasamy
Department of Mathematics
Indian Institute of Technology, Madras
Chennai - 600 036, India.
E-mail: vasantak@md3.vsnl.net.in

Abstract: *In this paper we study the notion of Smarandache-Galois fields and homomorphism and the Smarandache quotient ring. Galois fields are nothing but fields having only a finite number of elements. We also propose some interesting problems.*

Keywords: *Smarandache ring, Smarandache-Galois field, Smarandache field homomorphism, Smarandache quotient ring*

Definition [2]: *The Smarandache ring* is defined to be a ring A such that a proper subset of A is a field (with respect with the same induced operations). By proper set we understand a set included in A, different from the empty set, from the unit element if any, and from A.

Definition 1: A finite ring S (i.e. a ring having finite number of elements) is said to be a *Smarandache-Galois field* if S contains a proper subset A, $A \subset S$ such that A is a field under the operations of S.

Clearly we know every finite field is of characteristic p and has p^n elements, $0<n<\infty$.

Example 1: Let $Z_{10} = \{0, 1, 2, 3, 4, 5, ..., 9\}$ be the ring of integers modulo 10. Z_{10} is a Smarandache-Galois field. For the set $A = \{0, 5\}$ is a field for $5^2 = 5$ acts as a unit and is isomorphic with Z_2.

Example 2: Let $Z_8 = \{0, 1, 2, ..., 7\}$ be the ring of integers modulo 8. Z_8 is not a Smarandache-Galois field, for Z_8 has no proper subset A which is a field.

Thus we have the following interesting theorem.

Theorem 2: Z_{p^n} is not a Smarandache field for any prime p and for any n.

Proof: Z_{p^n} is the ring of integers modulo p^n. Clearly Z_{p^n} is not a field for $p^r.p^s = 0 \pmod{p^n}$ when $r + s = n$. Now any $q \in Z_{p^n}$ if not a multiple of p will generate Z_{p^n} under the operations addition and multiplication. If q is a multiple of p (even a power of p) then it will create zero divisors. So Z_{p^n} cannot have a proper subset that is a field.

Theorem 3: Let Z_m be the ring of integers modulo m. $m = p_1 \ldots p_t$, $t > 1$, where all p_i are distinct primes. Then Z_m is a Smarandache-Galois field.

Proof: Let Z_m be the ring of integers modulo m. Let $m = p_1 \ldots p_t$, for every prime p_i under addition and multiplication will generate a finite field. So Z_m is a Smarandache-Galois field.

Example 3: Let $Z_6 = \{0, 1, 2, \ldots, 5\}$. Clearly $\{0, 2, 4\}$ is a field with $4^2 = 4$ (mod 6) acting as the multiplicative identity. So $\{0, 2, 4\}$ is a field. Similarly $\{0, 3\}$ is a field. Hence Z_6 is a Smarandache-Galois field.

Example 4: Let $Z_{105} = \{0, 1, 2, \ldots, 104\}$be the ring of integers modulo 105. Clearly $A = \{0, 7, 14, 21, 28, \ldots, 98\}$ is a field with 15 elements. So Z_{105} is a Smarandache-Galois field.

Example 5: Let $Z_{24} = \{0, 1, 2, \ldots, 23\}$ be the ring of integers modulo 24. $\{0, 8, 16\}$ is a field with 16 as unit since $16^2 = 16$ and $\{0, 8, 16\}$ isomorphic with Z_3. So Z_{24} is a Smarandache-Galois field.

Note that $24 = 2^3.3$ and not of the form described in Theorem 3.

Example 6: $Z_{12} = \{0, 1, 2, \ldots, 11\}$. $A = \{0, 4, 8\}$ is a field with $4^2 = 4$ (mod 12) as unit. So Z_{12} is a Smarandache-Galois field.

Theorem 4: Let Z_m be the ring of integers with $m = p_1^{\alpha_1} p_2$. Let $A = \{ p_1^{\alpha_1}, 2p_1^{\alpha_2}, \cdots, (p_2 - 1)p_1^{\alpha_1}, 0\}$. Then A is a field of order p_2 with $p_1^{\alpha_i} . p_1^{\alpha_i} = p_1^{\alpha_i}$ for some α_i and $p_1^{\alpha_i}$ acts as a multiplicative unit of A.

Proof: Let Z_m and A be as given in the theorem. Clearly A is additively and multiplicatively closed with 0 as additive identity and $p_1^{\alpha_i}$ as multiplicative identity.

We now pose the following problems:

Problem 1: Z_m is the ring of integers modulo m. If $m = p_1^{\alpha_1}, \ldots, p_t^{\alpha_t}$ with one of $\alpha_i = 1$, $1 \leq i \leq t$. Does it imply Z_m has a subset having p_i elements which forms a field?

Problem 2: If Z_m is as in Problem 1, can Z_m contain any other subset other than the one mentioned in there to be a field?
Further we propose the following problem.

Problem 3: Let Z_m be the ring of integers modulo m that is a Smarandache-Galois field. Let $A \subset Z_m$ be a subfield of Z_m. Then prove $|A|/m$ and $|A|$ is a prime and not a power of prime.
A natural question now would be: Can we have Smarandache-Galois fields of order p^n where p is a prime? When we say *order of the Smarandache-Galois field* we mean only the number of elements in the Smarandache Galois field. That is like in Example 3 the order of the Smarandache-Galois field is 6. The answer to this question is yes.

Example 7: Let $Z_p[x]$ be the polynomial ring in the variable x over the field Z_p (p a prime). Let $p(x) = p_o + p_1x + \ldots + p_nx^n$ be a reducible polynomial of degree n over Z_p. Let I be the ideal generated by p(x) that is $I = \langle p(x) \rangle$.

Now $\dfrac{Z_p[x]}{I = \langle p(x) \rangle} = R$ is a ring.

Clearly R has a proper subset A of order p which is a field. So their exists Smarandache-Galois field of order p^n for any prime p and any positive integer n.

Example 8: Let $Z_3[x]$ be the polynomial ring with coefficients from the field Z_3. Consider $x^4 + x^2 + 1 \in Z_3[x]$ is reducible. Let I be the ideal generated by $x^4 + x^2 + 1$. Clearly $R = \dfrac{Z_3[x]}{I} = \{I, I + 1, I + 2, I + x, I + 2x, I + x + 1, I + x + 2,$ $I + 2x + 1, I + 2x + 2, I + x^2, I + x^3, \ldots, I + 2x + 2 + 2x^2 + 2x^3\}$ having 81 elements . Now
$\{ I, I + 1, I + 2 \} \subseteq R$ is a field. So R is a Smarandache-Galois field of order 3^4.

Theorem 5: A finite ring is a Smarandache ring if and only if it is a Smarandache-Galois field.

Proof: Let R be a finite ring that is a Smarandache ring then, by the very definition, R has a proper subset which is a field. Thus R is a Smarandache-Galois field.
Conversely, if R is a Smarandache-Galois field then R has a proper subset which is a field. Hence R is a Smarandache ring.

This theorem is somewhat analogous to the classical theorem "Every finite integral domain is a field" for "Every finite Smarandache ring is a Smarandache-Galois field".

Definition 6: Let R and S be two Smarandache-Galois fields. ϕ, a map from R to S, is a *Smarandache-Galois field homomorphism* if ϕ is a ring homomorphism from R to S.

Definition 7: Let R and S be Smarandache Galois fields. We say ϕ from R to S is a *Smarandache-Galois field isomorphism* if ϕ is a ring isomorphism from R to S.

Definition 9: Let Z_m be a Smarandache field. $A \subset Z_m$ be a subfield of Z_m. Let $r \in A$ such that $r \neq 0$, $r^2 = r \pmod{m}$ acts as the multiplicative identity of A. Define $\frac{Z_m}{\{A\}} = \{0,1,2, \ldots, r-1\}$. We call $\frac{Z_m}{\{A\}}$ the *Smarandache quotient ring* and the operation on $\frac{Z_m}{\{A\}} = \{0,1,\ldots, r-1\}$ is usual addition and multiplication modulo r.

Theorem 9: Let Z_m be a Smarandache-Galois field. $A \subset Z_m$ be a subfield of Z_m. $\frac{Z_m}{\{A\}}$ the Smarandache quotient ring need not in general be a Smarandache ring or equivalently a Smarandache-Galois field.

Proof: By an example. Take $Z_{24} = \{0, 1, 2, \ldots, 23\}$ be the ring of integers modulo 24. Let $A = \{0, 8, 16\}$; $16^2 = 16 \pmod{24}$ acts as multiplicative identity for A. $\frac{Z_{24}}{\{A\}} = \{0, 1, 2, \ldots, 15\}$. Clearly $\frac{Z_{24}}{\{A\}}$ is not a Smarandache ring or a Smarandache-Galois field.

Thus, motivated by this we propose the following:

Problem 4: Find conditions on m for Z_m to have its Smarandache quotient ring to be a Smarandache ring or Smarandache-Galois field.

Example 10: $Z_{12} = \{0, 1, \ldots, 11\}$ is the ring of integers modulo 12. $A = \{0, 4, 8\}$ is a field with $4^2 = 4 \pmod{12}$ as multiplicative identity. $\frac{Z_{12}}{\{0,4,8\}} = \{0, 1, 2, 3\} \pmod 4$ is not a Smarandache-Galois field or a Smarandache ring.

Example 11: $Z_{21} = \{0, 1, 2, \ldots, 20\}$ is the ring of integers modulo 21. $A = \{0, 7, 14\}$ is a subfield. $\frac{Z_{21}}{\{A\}} = \{0,12,\ldots,6\} \bmod 7$ is not a Smarandache-Galois field. Let $B = \{0,3,6,9,12,15,18\} \subseteq Z_{21}$. Clearly B is a field with $15^2 = 15 \pmod{21}$

as a multiplicative unit. Now, $\frac{Z_{21}}{\{0,3,6,9,12,15,18\}} = \{0,1,2,\ldots,14\}$ is a Smarandache-Galois field.

Thus we have the following interesting:

Problem 5: Let Z_m be the Smarandache ring. Let A be a subset which is a field. When does an A exist such that $\frac{Z_m}{A}$ is a Smarandache-Galois field?

References:

[1] I. N. Herstein, *Topics in Algebra*, New York, Blaisdell, 1964.

[2] Padilla, Raul. *Smarandache Algebraic Structures,* Bulletin of Pure and Applied Sciences, Delhi, Vol. 17 E., No. 1, 119-121, 1998; http://www.gallup.unm.edu/~smarandache/ALG-S-TXT.TXT .