COMPOSITIO MATHEMATICA

YOUSIF AL-KHAMEES

The intersection of distinct Galois subrings is not necessarily Galois

Compositio Mathematica, tome 40, nº 3 (1980), p. 283-286

<http://www.numdam.org/item?id=CM_1980__40_3_283_0>

COMPOSITIO MATHEMATICA, Vol. 40, Fasc. 3, 1980, pag. 283–286

THE INTERSECTION OF DISTINCT GALOIS SUBRINGS IS NOT NECESSARILY GALOIS

Yousif Al-Khamees

All the rings considered in this paper are finite, have an identity, subrings contain the identity and ring homomorphism carry identity to identity. By a "completely primary ring" we mean precisely a ring R in which the set J of all zero divisors of R forms an additive group. It is well known that if R is a completely primary ring, then $|R| = p^{nr}$, $|J| = p^{(n-1)r}$, $R/J \cong GF(p^r)$, the Galois field of order p^r and the char of R is p^k, where $1 \leq k \leq n$, for some prime p and positive integers n, r, k.

Of special interest is the case $k = n$; in this case they are commutative and isomorphic to $Z_{p^k}[X]/(f)$, where Z_{p^k} is the ring of integers modulo p^k, and $f \in Z_{p^k}[X]$ is monic irreducible mod p and of degree r. These rings were first considered by Krull (1924), [4] and since then rediscovered by others. Following the general trend, we call such a ring a Galois ring and denote it by $GR(p^{kr}, p^k)$.

In [6], proposition (1), Raghavendran stated that subrings of Galois rings are Galois. This is not true in general, as example (1) below shows. A trivial, alas false, consequence of this is that the intersection of Galois subrings of a ring is Galois. These are minor flaws in themselves, but since they have now been repeated in [5] and [7], we think it appropriate to publish this little note to prevent further misuse.

In this note we also provide necessary and sufficient conditions for subrings of Galois rings to be Galois and for the intersections of Galois subrings to be Galois.

We need the following lemma.

LEMMA (1): *Let R be a completely primary ring, then R is Galois iff $J = pR$.*

0010–437X/80/03/0283–04$00.20/0

This is lemma (2) of [2].

EXAMPLE (1): Let R be a Galois ring of the form $GR(p^{kr}, p^k)$. Consider the subring $Z_{p^k}[J]$ of R. Since the residue field of $Z_{p^k}[J]$ is Z_p, the order of $Z_{p^k}[J]$ is $p^{(k-1)r+1}$. This subring is Galois only when $(k-1)r+1=k$; this implies $(r-1)(k-1)=0$, so $r=1$ or $k=1$ or both. Therefore $Z_{p^k}[J]$ is not Galois if $k>1$ and $r>1$. So subrings of a Galois ring are not necessarily Galois.

This example is due to B. Corbas.

EXAMPLE (2): Let $R_0 = Z_4[X]/(X^2+X+1) = Z_4[a]$, where $a = X+(X^2+X+1)$; clearly R_0 is a Galois ring of the form $GR(2^{2\cdot 2}, 2^2)$, a is of multiplicative order 3, and $K = GF(2^2)$ is the residue field of R_0. In the construction (A) given in [3], take $R_0 = R_0$, $V = K$ and $\phi: K \mapsto \mathrm{End}_K K \cong K$

$$x \mapsto x^2.$$

So the multiplication defined on $R = R_0 \oplus K$ as follows

$$(r_0, r_1)(s_0, s_1) = (r_0 s_0 + \psi(r_0)s_1 + (\psi(s_0))^2 r_1),$$

where $\psi: R_0 \to K$ is the canonical homomorphism, makes R into a ring.

Obviously $R_1 = (R_0, 0)$ is a Galois subring of R of the form $GR(2^{2\cdot 2}, 2^2)$. Let $R_2 = (a,1)R_1(a,1)^{-1} = (a,1)R_1(a^2,1)$, then clearly R_2 is also a Galois subring of R of the form $GR(2^{2\cdot 2}, 2^2)$. Now $(a,1)(a,0)(a,1)^{-1} = (a,1)(a,0)(a^2,1) = (a^2,a^2)(a^2,1) = (a, a^2+1) = (a,a) \notin R_1$, this implies that $R_1 \neq R_2$, hence $|R_1 \cap R_2| < 2^{2\cdot 2} = 16$. On the other hand $(a,1)(2a,0)(a,1)^{-1} = (a,1)(2a,0)(a^2,1) = (2a^2,0)(a^2,1) = (2a,0) \in R_1 \cap R_2$, so $|R_1 \cap R_2| \geq 8$, and hence $|R_1 \cap R_2| = 8$. If $R_1 \cap R_2$ is Galois then $|R_1 \cap R_2| = 8 = 2^{2r}$, where r is a positive integer, contradiction. So $R_1 \cap R_2$ is not Galois.

It is not difficult to see that the above example can be generalized as follows.

Let R be a non-commutative completely Primary ring of char p^k *such that $p^i R = p^i R_0$, where $i \leq k-1$, and R_0 is a maximal Galois subring of R, then the intersection of any distinct maximal Galois subrings of R is not Galois.*

There are numerous rings satisfying these conditions, for instance the rings of char p^2 given by construction (A) in [3].

PROPOSITION (1): *Let R be a completely Primary ring of* char p^k, *then R is Galois iff R is Principal and $J^k = 0$.*

PROOF: Assume that R is principal, $J^k = 0$ and $|R/J| = p^r$ where r is a positive integer. Since R is principal, $\dim_{R/J}(J/J^2) \leq 1$, but $J \neq J^2$, otherwise J is not nilpotent, so $\dim_{R/J}(J/J^2) = 1$, and hence $|J/J^2| = p^r$. Now consider the map

$$J^i/J^{i+1} \longrightarrow J^{i+1}/J^{i+2}$$

$$x + J^{i+1} \xrightarrow{\phi} px + J^{i+2}.$$

It is easily seen that ϕ is a surjective R/J – linear mapping , therefore, $\dim_{R/J}(J^i/J^{i+1}) \leq 1$ for all i; hence $p^{nr} = |R| \leq p^{kr}$, so $n = k$ and, therefore, R is Galois.

COROLLARY (1): *A subring of a Galois ring is Galois iff it is principal.*

COROLLARY (2): *The intersection of any two Galois subring is Galois iff it is principal.*

The correct version of proposition (1) *of* [6] *becomes now*

Let R be a Galois ring of the form $GR(p^{kr}, p^k)$; then R has a Galois subring of the form $GR(p^{ks}, p^k)$ iff $s \mid r$.

This is easy to prove considering the restriction of the canonical homomorphism $R \to R/J$ to the relevant subring.

Acknowledgement

The author wishes to express his gratitude and indebtedness to Dr. B. Corbas, for stimulating his interest in finite rings and for his helpful discussions during the preparation of this paper.

REFERENCES

[1] M.F. ATIYAH and I.G. MACDONALD: *Introduction to commutative Algebra.* Addison-Wesley Publ. (1969).
[2] W.E. CLARK: A coefficient ring for finite non-commutative rings, *Proc. Amer. Math. Soc. 33*, No. 1 (1972) 25–27.
[3] B. CORBAS: Finite rings in which the product of any two zero divisors is zero. *Archiv der Math., XXI* (1970) 466–469.
[4] W. KRULL: Algebraische theorie der ringe 11. *Math. Ann. 91* (1924) 1–46.
[5] R.G. MACDONALD, *Finite rings with identity*, Dekker, New York (1974).
[6] R. RAGHAVENDRAN: Finite Associative rings, *Compositio Math. 21*, 2 (1969) 195–229.
[7] R. WILSON: On the structure of finite rings, *Compositio Math. 26*, 1 (1973) 79–93.

(Oblatum 24-V-1976 & 13-VI-1979)

Department of Mathematics,
Faculty of Science,
University of Riyadh,
Riyadh,
Saudi Arabia