BULLETIN OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 78, Number 6, November 1972

GALOIS SUBRINGS OF ORE DOMAINS ARE ORE DOMAINS

BY CARL FAITH

Communicated by Nathan Jacobson, April 24, 1972

If R is a ring, and G is a group of automorphisms of R, then R^G denotes the subring of R consisting of elements of R left fixed by every element of G, and is called the *Galois subring corresponding to* G. In his paper, *Groups acting on hereditary rings*, G. M. Bergman has asked if every Galois subring of a right Ore domain corresponding to a finite group is itself right Ore. In this note we show that the answer is affirmative.

Henceforth, let R denote a right Ore domain with right quotient field D, let G be a finite group of automorphisms, and let $G' = \operatorname{ex} G$ denote the unique extension of G to D. Then, $G' \approx G$ under the restriction map $g' \mapsto g$.

Henceforth, we let G denote a group of automorphisms of D which induces a group of automorphisms of R isomorphic to G under the canonical map. We borrow a term from ring theory coined for another use: the Galois subring R^G will be said to be *right quorite* in case R^G is a right Ore domain with right quotient field $= D^G$. The theorem we prove is slightly stronger than that stated in the title.

THEOREM. *If G is a finite group of automorphisms of a right Ore domain R, then R^G is right quorite.*

Our proof depends heavily on the Cartan-Jacobson Galois theory for division rings, including Jacobson's outer Galois theory of an earlier paper, and concomitant normal basis theorems of Nakayama, Kasch, Tominaga, and the author in the special case when $[D:D^G] = (G:1)$.

Successive reductions for the truth of the theorem can be made to the cases (i) G is an outer or inner group of automorphisms of D (Lemma 1), (ii) G is simple (Lemma 1), (iii) R has prime characteristic p dividing $(G:1)$ (Lemma 2), (iv) G is inner (Lemma 4), and finally, (v) G is cyclic of order p (Lemma 5, ff.).

Both (i) and (ii) are obtained as corollaries of the following lemma:

LEMMA 1. *Assume that there is a subnormal series*

$$G = G_0 \supset G_1 \supset \ldots \supset G_{m-1} \supset G_m = 1. \tag{1}$$

AMS 1970 *subject classifications.* Primary 16A08, 16A40, 16A72, 16A74; Secondary 13B05.

Key words and phrases. Integral domain, Ore domain, quotient field, finite automorphism group, Galois subring, Galois theory, Cartan-Jacobson Galois theory, Nakayama-Kasch normal basis theorem, Faith-Tominaga normal basis theorem, outer automorphisms, trace function, fields, quasi-fields, unit group, commutator subgroup, simple group, division rings.

If the theorem holds for all groups of automorphisms isomorphic to any factor group G_i/G_{i+1}, $0 \leqq i \leqq m-1$, *then the theorem holds for any group of automorphisms isomorphic to* G.

By induction on m, it suffices to consider the case $m = 2$. By normality of G_2 in G_1, the group G induces a group $\bar{G}_1$ of automorphisms of D^{G_1} canonically isomorphic to G/G_1. An induction hypothesis on the order of the group permits the assumption that R^{G_1} is right quorite with right quotient field D^{G_1}, and the same hypothesis then implies that $(R^{G_1})^{\bar{G}_2} = R^{G_2}$ is right quorite, with right quotient field $(D^{G_1})^{\bar{G}_2} = D^{G_2}$. □

(i) is obtained as the $m = 2$ case, with G_1 denoting the group of inner automorphisms of G. Moreover, (ii) is the case for which (1) is a composition series for G.

The outer case. We let $Q(A)$ denote the right quotient field of any right Ore domain A. We also let $t: D \to F$ denote the trace function defined by G, where $F = D^G$. The restriction of t to R is a mapping $R \to R^G$ also denoted by t. We assume throughout that R is a right Ore domain and that G is a finite group of automorphisms. We also let p denote the characteristic of R, possibly $p = 0$.

Lemma 2. *If the G-trace function does not vanish on R, then* R^G *is right quorite. A sufficient condition for this is for p to be prime to* $(G:1)$.

Proof. To show that $A = R^G$ is right Ore it is required to show for any nonzero $x, y \in A$ that there exist $x_1, y_1 \in A$ such that $y^{-1}x = x_1 y_1^{-1}$. Since D is the right quotient field of R, there do exist elements x_1, y_1 in R with this property, and furthermore,

$$t(x_1 a)t(y_1 a)^{-1} = y^{-1}x \tag{2}$$

for any $a \in R$ such that $t(y_1 a) \neq 0$.

Assume $t(y_1 R) = 0$. By the Galois theory of division rings of Cartan [**48**]-Jacobson [**47**] (cf. Jacobson [**64**]), D is a left (and right) vector space over F of dimension $m \leqq n = (G:1)$. If $u_1, \dots, u_m$ is a left F-basis, then the fact that $y_1 R$ is an essential right ideal of R implies that there exists a nonzero element $b \in R$ such that $w_i = u_i b \in y_1 R$, $l = 1, \dots, m$. It follows that $w_1, \dots, w_m$ are left F-independent, and, moreover,

$$D = \sum_{i=1}^{m} F w_i = \sum_{i=1}^{m} F u_i b = Db = D.$$

Thus, for any $d \in D$, there exist elements $d_i \in F$, $i = 1, \dots, m$, such that

$$d = \sum_{i=1}^{m} d_i w_i,$$

and hence,

$$t(d) = \sum_{i=1}^{m} d_i t(w_i) = 0.$$

This proves that t vanishes on D, hence on R, contrary to the assumption. (Since $t(1) = n$, then t vanishes on R only if $p|n$.) Thus, we have the desired equality (2) for some $a \in R$. This proves that A is right Ore. Moreover, the proof actually shows that any $z \in F$ can be written $z = t(x_1 a)t(y_1 a)^{-1}$, for some $a \in R$, where x_1 and y_1 are elements of R such that $z = x_1 y_1^{-1}$. This proves that $Q(A) = F$, hence that A is right quorite. □

Let $[D:F]$ denote the left dimension of D over F, where $F = D^G$. We say that D has a *G-normal basis* if $[D:F] = (G:1)$ and if there is an element $u \in D$ such that $\{u^g\}_{g \in G}$ is a left basis of D over F.

THEOREM 3 (FAITH [**58**], TOMINAGA [**58**]). *If $[D:F] = (G:1)$, then D has a G-normal basis element u, and hence the G-trace function is nonvanishing.* □

LEMMA 4. *If G is a finite group of automorphisms of a right Ore domain R canonically extended to an outer group of automorphisms of D, then $A = R^G$ is right quorite.*

PROOF. As shown first by Jacobson [**40**] in the case of noncommutative division rings (called quasi-fields in [**40**]), the condition $[D:F] = (G:1)$ holds whenever G is an outer group of automorphisms of D. In this case, the normal basis theorem for noncommutative D is a theorem of Nakayama [**40**] (cf. Kasch [**53**]). □

The inner case. If D is a division ring, D^* will represent its group of units, and $[H, H]$ the commutator subgroup of any group H.

LEMMA 5. *Let D be a division ring of characteristic p, and G a finite group of inner automorphisms of D. Then $[G, G]$ contains no elements of order p.*

PROOF. Let C denote the center of D; thus G may be identified with a subgroup of D^*/C^*. If we choose a representative in D for each element of G, these will span over C a subalgebra D_0 of finite dimension m, which we may represent by $m \times m$ matrices over C. Clearly, any element $g \in [G, G]$ may be represented by an element $x \in [D_0^*, D_0^*]$, and as a matrix, x will have determinant 1. Hence if $x^p \in C^*$, we get $1 = \det(x^p) = x^{pm}$. So x is algebraic over the prime field $P = \mathrm{GF}(p) \subseteq C$, so $P(x)$ is finite, hence perfect, hence $P(x) = P(x^p) \subseteq C$. Hence $x \in C^*$, and the element $g \in [G, G]$ represented by x is the identity. □

Now by our previous reductions, all that remains to prove of the theorem is the case where G is a simple group of inner automorphisms of D, of order divisible by p. By simplicity, $[G, G]$ is either equal to G or trivial. By the above lemma the latter must hold, so G must be abelian, of order p. We now prove that the trace function t is nonvanishing, so that R^G is quorite by Lemma 2.

Let a generator of the cyclic group G be represented by $x \in D^*$. Then $x^p = a \in C^*$, so $\lambda^p - a$ is the minimal polynomial of x over C (cf. Albert [47, p. 188]). Hence $[C(x):C] = p$. By the inner Galois theory, $C(x)$ is the centralizer of F in D, and $[D:F] = [C(x):C] = p = (G:1)$, so by Theorem 3, t is nonvanishing.[1]

References

47. A. A. Albert, *Modern higher algebra*, Univ. of Chicago Press, Chicago, Ill., 1947.

71. G. M. Bergman, *Groups acting on hereditary rings*, Proc. London Math. Soc. (3) **23** (1971), 70–82.

48. H. Cartan, *Théorie de Galois pour les corps non commutatifs*, Ann. Sci. École Norm. Sup. (3) **64** (1947), 59–77. MR **9**, 325.

58. C. C. Faith, *Galois extensions in which every element with regular trace is a normal basis element*, Proc. Amer. Math. Soc. **9** (1958), 222–229; correction, **11** (1960), 670. MR **20** #2357; MR **22** #8007.

40. N. Jacobson, *The fundamental theorem of the Galois theory for quasi-fields*, Ann. of Math. (2) **41** (1940), 1–7. MR **1**, 198.

47. ———, *A note on division rings*, Amer. J. Math. **69** (1947), 27–36. MR **9**, 4.

64. ———, *Structure of rings*, rev. ed., Amer. Math. Soc. Colloq. Publ., vol. 37, Amer. Math. Soc., Providence, R.I., 1964. MR **36** #5158.

53. F. Kasch, *Über den Endomorphismring eines Vektorraumes und den Satz von der Normalbasis*, Math. Ann. **126** (1953), 447–463. MR **15**, 597.

40. T. Nakayama, *Normal basis of a quasi-field*, Proc. Imp. Acad. Tokyo **16** (1940), 532–536. MR **2**, 344.

58a. H. Tominaga, *A note on Galois theory of primary rings*, Math. J. Okayama Univ. **8** (1958), 117–123. MR **21** #4172.

58b. ———, *On the normal basis theorem and strictly Galois extensions*, Math. J. Okayama Univ. **8** (1958), 133-142.

Department of Mathematics, Rutgers, The State University, New Brunswick, New Jersey 08903

[1] Added February 4, 1972. I am indebted to George M. Bergman for showing me that my proof of Lemma 5 leads to the stated (stronger) conclusion, and also for pointing out that the nonvanishing of t can be proved by a result of Bergman and Isaacs in an unpublished paper, *Rings with fixed-point free group actions* [J. London Math. Soc. (to appear)]. (They show that if a cyclic p-group G acts faithfully on a ring R of characteristic p so that the trace function vanishes, then R has nonzero nilpotent elements. Hence in this case, t cannot vanish.