GALOIS EXTENSIONS OF COMMUTATIVE RINGS

CARL FAITH

Introduction. Let R be any ring, let G be a group of automorphisms of R, and let A denote the fixring $R^G = \{r \in R \mid g(r) = r \text{ for all } g \in G\}$. Then we say that R is *Galois* over A.

Next assume that R is a *right Ore ring*, that is, that R has a right quotient ring $Q = Q(R) = \{ab^{-1} \mid a, \text{ regular } b \in R\}$ in which every regular element of R is a unit. As Ore [2] showed, a necessary and sufficient condition for this is that for all $a \in R$ and regular $b \in R$ there exist $a_1 \in R$ and regular $b_1 \in R$ such that $ab_1 = ba_1$. Thus, any commutative ring is right Ore; an integral domain which is right Ore is called a *right Ore domain.*

If R is right Ore, then each $g \in G$ has a unique extension to an automorphism $\mathrm{ex}\, g$ of $Q(R)$, and the correspondence

$$g \longmapsto \mathrm{ex}\, g$$

is an isomorphism of G with the extended group $\mathrm{ex}\, G = \{\mathrm{ex}\, g \mid g \in G\}$. Henceforth let us identify the two groups, and set $F = Q^G = \{ab^{-1} \in Q \mid g(ab^{-1}) = ab^{-1} \text{ for all } g \in G\}$. We say that the pair (R, G) is right *quotient-right* (*quorite*, for short) in case $A = R^G$ is a right Ore ring with right quotient ring $F = Q^G$. In my paper [1], I showed that (R, G) is right quorite for any right Ore domain, and finite group G of automorphisms. In the proof, the hard part was to prove that A is actually right Ore, and then $Q(A) = F$ is an easy consequence. At that time, I made no reference to the case R commutative because any commutative domain is an Ore domain.

Let us consider now the "problem" of which pairs (R, G) are quorite when R is commutative. Note that a necessary condition for (R, G) to be quorite is for an embedding $Q(A) \hookrightarrow Q(R)$ of rings. As we show, this can happen if and only if the canonical module R_A is *torsion free* in the sense that each $a \in A$ which is regular in A is regular in R. An example when R_A is not torsion free, discovered by J. Koehl, is the factor ring R of the polynomial ring $S = k[x_1, x_2, x_3]$ over a field k modulo the ideal $I = (x_1x_2, x_1x_3, x_2x_3, x_2 + x_3)$. Let G be the cyclic group (g) of order 2 which interchanges x_2 and x_3 and leaves x_1 fixed. Then the fixring is $A = k[\bar{x}_1]$, which has a regular element $\bar{x}_1$ not regular in R, where $\bar{f}$ denotes the image of any polynomial f under the canonical map. Thus, $\bar{x}_1\bar{x}_2 = \bar{x}_1\bar{x}_3 =$

0. By taking the power series ring $k\langle x_1, x_2, x_3\rangle = S$ we can find an example $R=S/I$ which is a local ring with R_A not torsion free.

The fact that the counterexample to the quotient-rightness of all pairs (R, G) is so simple, indicates the problem is not well-stated. Even so, one might ask what assumptions on G or R imply that (R, G) is quotient-right. Inasmuch as the example above can be modified to include all cyclic groups (finite or not) then one could expect that G would have to be highly noncommutative.

Ordinarily, in the commutative Galois theory of Auslander-Goldman, or Chase-Harrison-Rosenberg, the situation for (R, G) is that R_A is finitely generated projective (and even further demands are placed on the extension so that $\mathrm{End}_A R$ is generated by G and the homothetics r_a by elements $r \in R$). In contrast, when G is finite, for (R, G) to be quorite, we require only that R_A be torsion free (Theorem 2), hence R_A flat suffices. As a consequence, (R, G) is quorite when R has no nilpotent ideals. Thus (R, G) is quorite whenever R is semihereditary.

We have indicated even for finite G that right quotient-rightness of R is not a "natural" phenomenon, while at the same time gave some sufficient conditions for it. We have saved for last the statement of perhaps our main theorem which states in *every* case $F=Q^G$ is the partial right quotient ring of $A=R^G$ with respect to the multiplicative set S of all elements $a \in A$ which are regular in R (Theorem 1). Thus, the condition $F=A_S$ is *the* natural one.

Theorems. As stated, R will be a commutative ring with identity, and $Q=Q(R)$ the full quotient ring. Let G be a group of automorphisms of Q which induces a group of automorphisms of R isomorphic to G under the canonical map. Then we set $F=Q^G$, and $A=R^G=F\cap R$. The orbit $Gx=\{g(x) \mid g\in G\}$ is assumed to be finite for any element $x\in Q$.

For future reference, we let T^* be the set of regular elements, and $N(T)$ the set of nilpotent elements of any ring T.

Given an element $x\in Q$ with $n=|Gx|$, we consider the monic polynomial

$$f_x(X)=\prod_{Gx}(X-g(x))=X^n+a_1X^{n-1}+\cdots+a_{n-1}X+a_n$$

in $F[X]$. It is obvious that $f_x(x)=0$. In particular, if $x\in R$ then $f_x(X)\in A[X]$, and x is integral over A. Furthermore, if $x\in R^*$ then a_n is a unit in Q, and

$$x^{-1}=(-x^{n-1}-a_1x^{n-2}-\cdots-a_{n-1})a_n^{-1}.$$

Now, let $x \in a^{\perp} = \{y \in R \mid ay = 0\}$ for a regular element a of A. Then $a_i \in a^{\perp} \cap A = 0$ $(i = 1, \cdots, n)$ and $x^n = -(a_1 x^{n-1} + \cdots + a_n) = 0$, namely, $a^{\perp}$ is a nil ideal.

Summarizing the above, we have the following

Lemma. (1) *R is integral over A.*

(2) *If $x \in R^*$ then $x^{-1} = rs^{-1}$ with an element $r \in R$ and an element $s \in A$ which is a unit in Q.*

(3) *If $a \in A^*$ then $a^{\perp}$ is a nil ideal of R.*

Theorem 1. *F is the partial quotient ring A_S of A with respect to the multiplicative subset $S = \{a \in A \mid a^{-1} \in Q\} = A \cap R^*$. Moreover, $Q = RA_S = RF$.*

Proof. The partial quotient ring A_S embeds in Q under the map

$$a/s \longmapsto as^{-1} \quad (a \in A,\ s \in S).$$

By Lemma (2), $Q = RA_S$. Now, let $y \in F$. Since $Q = RA_S$, there exist $r \in R$, $a \in S$, and $y = ra^{-1}$. But then, $r = ya \in F \cap R = A$, so $F \subseteq A_S$. Clearly, however, $a^{-1} \in F$, so that $F = A_S$.

Theorem 2. *The pair (R, G) is quorite if and only if R_A is torsion free.*

Proof. The first part is obvious in view of Theorem 1: If R_A is torsion free, then $S = A^*$, so $F = Q(A)$ as needed.

Corollary. *The pair (R, G) is quorite under any of the following conditions:*

1) $N(R) = 0$.

2) *R is semihereditary.*

3) *R_A is flat.*

4) *R is a Galois extension of A in the sense of Chase-Harrison-Rosenberg.*

Proof. 1) follows from Lemma (3) and Theorem 2, and 2) implies 1). Also, any flat module is torsion free, so 3) follows from Theorem 2. Moreover, 4) follows from 3) (as mentioned in the introduction).

Remark. Corollary establishes quotient-rightness of (R, G) in the case $N(R)$ is as small as possible. On the other hand, we also get quotient-rightness (at least for local rings without any restriction) when $N(R)$ is as large as possible: If R is a local ring, with radical $N(R)$, then

(R, G) is quorite, and in fact $Q=R$, and $F=A$.

Conclusion. For any ring monic

$$0 \longrightarrow B \longrightarrow R \tag{1}$$

there is a ring monic

$$0 \longrightarrow Q(B) \longrightarrow Q(R)$$

if and only if R_B is torsion free. This certainly happens, for example, when $B=Q(B)$, or when R_B is flat, and in other instances. In this article, we have discussed only the instance when R/B is Galois corresponding to a group G under which each element of R has finite orbit. In some instances, for example, when R is a field, or when R is an algebraic algebra over a prime field, it will be true that $Q(B) \subseteq Q(R)$ for any subring $B \hookrightarrow R$. It would be interesting to classify those commutative rings R on which Q acts as a left exact functor (in the sense that (1) $\Longrightarrow$ (2)).

REFERENCES

[1] C. FAITH: Galois subrings of Ore domains are Ore domains, Bull. Amer. Math. Soc. **78** (1972), 1077—1080.
[2] O. ORE: Theory of non-commutative polynomials, Ann. of Math. **34** (1933), 480—508.

RUTGERS, THE STATE UNIVERSITY
NEW BRUNSWICK, NJ 08903, U. S. A.

(*Received September 16, 1975*)