76-24,370

ROARK, Charles Winfred, 1950-
SEPARABLE CRITERIA FOR G-DIAGRAMS
OVER COMMUTATIVE RINGS.

The University of Oklahoma, Ph.D., 1976
Mathematics

THE UNIVERSITY OF OKLAHOMA

GRADUATE COLLEGE

# SEPARABLE CRITERIA FOR G-DIAGRAMS OVER COMMUTATIVE RINGS

A DISSERTATION

SUBMITTED TO THE GRADUATE FACULTY

in partial fulfillment of the requirement for the

degree of

DOCTOR OF PHILOSOPHY

BY

CHARLES WINFRED ROARK

Norman, Oklahoma

1976

SEPARABLE CRITERIA FOR G-DIAGRAMS OVER COMMUTATIVE RINGS

APPROVED BY

Andy Magid

Leonard R. Rubin

Harold V. Huneke

DISSERTATION COMMITTEE

ACKNOWLEDGMENTS

This thesis was prepared under the supervision of Dr. Andy Roy Magid, who suggested the topic and whose help and assistance are gratefully acknowledged.

The encouragement and support given by my wife, Meredith, are also greatly appreciated.

## TABLE OF CONTENTS

## TABLE OF SYMBOLS

Let $S$ be a commutative ring with identity, $\Gamma$ and $G$ subgroups of the ring automorphisms of $S$ with $\Gamma$ finite, $F$ and $T$ fields, and $V$ a variety over an algebraically closed field $k$. The following is a list of symbols used in the text.

$C(\Gamma, S)$ = Ring of functions from $\Gamma$ to $S$.

$\mathrm{Spec}(S)$ = Prime ideals of $S$.

$\mathrm{Max}(S)$ = Maximal ideals of $S$.

$S^G = \{s \text{ in } S \mid g(s) = s \text{ for all } g \text{ in } G\}$.

$\mathrm{nilrad}(S) = \bigcap_{P \text{ in } \mathrm{Spec}(s)} P$.

$\mathrm{JRad}(S) = \bigcap_{M \text{ in } \mathrm{Max}(S)} M$.

$\mathbb{R}$ = Real numbers.

$\mathbb{C}$ = Complex numbers.

$Q$ = Rational numbers.

$\dim_T F$ = dimension of $F$ over $T$.

$k[V]$ = coordinate ring of $V$.

SEPARABLE CRITERIA FOR G-DIAGRAMS

OVER COMMUTATIVE RINGS

## INTRODUCTION

Throughout $S$ and $R$ are commutative rings with identity.

Let $k$ be an algebraically closed field, $V$ and $W$ affine algebraic sets, $G$ an affine group acting on $V$ and $W$, and $V_o$ and $W_o$ strict quotients of $V$ and $W$ respectively. If there exists a surjective $G$-morphism from $V$ to $W$, then we have

$$\begin{tikzcd} V \arrow[r] \arrow[d, dash] & W \arrow[d, dash] \\ V_o \arrow[r] & W_o \end{tikzcd}$$

with all maps surjective $G$-morphisms. This induces a diagram of inclusions on their coordinate rings:

$$\begin{tikzcd} & k[V] \arrow[dl, dash] \arrow[dr, dash] & \\ k^G[V] = k[V_o] \arrow[dr, dash] & & k[W] \arrow[dl, dash] \\ & k^G[W] = k[W_o] & \end{tikzcd}$$

The above motivates:

*Definition 0.1*: Let $G$ be a subgroup of the ring automorphisms of $S$ such that $G$ restricted to $R$ pointwise is contained in the ring automorphisms of $R$. Thus we have the following diagram of inclusions:

$$\begin{tikzcd}
 & S \arrow[dl, dash] \arrow[dr, dash] & \\
S^G \arrow[dr, dash] & & R \arrow[dl, dash] \\
 & R^G &
\end{tikzcd}$$

Such a diagram is called a *G-diagram of $S$ over $R$*. And in the case that $S = R\cdot S^G$, we say that $S$ is *invariantly generated over $R$*.

Recall that $S$ is a separable $R$-algebra if $S$ is a projective $S\otimes_R S$-module [DI, P.40]. $S$ is a strongly separable $R$-algebra if $S$ is a separable $R$-algebra and a finitely generated and projective $R$-module. Note that if $S$ is a separable $R$-algebra and a projective $R$-module, then $S$ is a finite $R$-module [VZ', 1.1]. If $\Gamma$ is a finite group of automorphisms of $S$, we say $S$ is a Galois extension of $R$ with group $\Gamma$ if the Chase-Harrison-Rosenberg definition of a Galois extension is satisfied [CHR] and [DI, P.84]. This paper is concerned with answering the following question: Suppose that we have a $G$-diagram of $S$ over $R$ and $S$ is a strongly separable (Galois) extension of $R$. Is $S^G$ a strongly separable (Galois) extension of $R^G$? And we are concerned in the Galois part of the question only in Galois extensions $S$ of $R$ with group $\Gamma$ in which $\Gamma$ acts also as a group of automorphisms of $S^G$. So if $(S^G)^\Gamma$ is written, we assume that $\Gamma$ is also a group of automorphism of $S^G$. We begin in the first chapter by finding necessary conditions to the question: $R \cdot S^G$ must satisfy the condition with respect to $R$. Next, we ask the question for $R$ a finite product of fields. Except, here, we change the strongly separable question to a weakly Galois question. Recall that if $\Gamma$ is a finite group of automorphisms of $S$, then $S$ is a weakly Galois extension of $R$ with group $\Gamma$ if $S^\Gamma = R$ and $S$ is a strongly separable $R$-algebra [VZ'', 3.6]. By recent work of Kreimer [K] we can change the definition to $S^\Gamma = R$ and $S$ is a separable $R$-algebra. We will find that the weakly Galois question is always true if $R$ is a finite product of fields, but the Galois question is not always true.

To set the second chapter we need a few definitions. Let $M$ be a finite dimensional $k$-module and $G$ an affine group. Then $M$ is a rational $G$-module if there exists a representation $\rho: G \to GL(M)$ which is a $k$-homomorphism [F, 2.23, P.64]. If $M$ is infinite dimensional, then $M$ is a rational $G$-module if $M$ is the union of finite dimensional rational $G$-submodules. Note that a

G-submodule of a rational G-module is rational. G is linearly reductive if every rational G-module is completely reducible, i.e., if M is a rational G-module and N a G-submodule, then there exists a G-submodule N' of M with $M = N \oplus N'$ [F, 4.6, P.116]. In this chapter we ask the question relative to the following setting: We have a G-diagram of S over R with S and R finitely generated k-algebras and G is linearly reductive acting rationally on S. We find that S can be a Galois extension of R and $S^G$ a finite $R^G$-module, yet $S^G$ is not even a separable $R^G$-algebra. But we do find necessary and sufficient conditions for $S^G$ to be a separable (Galois) $R^G$-algebra.

SEPARABLE CRITERIA FOR G-DIAGRAMS

OVER COMMUTATIVE RINGS

# CHAPTER I

## GENERALITIES AND FIELD CASE

Unless explicitly noted to the contrary, all rings and algebras are assumed commutative with identity. All unadorned tensors will be clear from the context.

In this chapter the following are discussed: generalities needed in studying the problem, observations in the non-algebraic-geometric context, and the question with suitable restriction on R.

We begin by finding necessary conditions for $S^G$ to be a separable $R^G$-algebra and for $S^G$ to be a Galois extension of $R^G$. But first we recall the definition of a ring S being a Galois extension of R with finite group $\Gamma$ of R algebra automorphisms. Let

$$\ell\colon \quad S\otimes_R S \to C(\Gamma,S)$$

be defined by $\ell(\Sigma s\otimes t)(\gamma) = \Sigma s\gamma(t)$ for s and t in S and $\gamma$ in $\Gamma$. Then S is a Galois extension of R with group $\Gamma$ if $S^\Gamma = R$ and $\ell\colon S\otimes S \to C(\Gamma,S)$ is an isomorphism [DI, P.84].

But we can be less restrictive:

(1.1) $S$ is a Galois extension of $R$ with group $\Gamma$, if $S^{\Gamma} = R$ and $\ell$: $S \otimes S \to C(\Gamma, S)$ is surjective.

Proof: We show that (1.1) is equivalent to the following:

$$(*)\qquad \begin{array}{ll} \text{i.} & S^{\Gamma} = R \\ \text{ii.} & \text{There exists } x_1, \ldots, x_n, y_1, \ldots, y_n \\ & \text{in } S \text{ such that } \Sigma x_i \gamma(y_i) = \delta_{\gamma,1}. \end{array}$$

((*) is one of the equivalent definitions for $S$ to be a Galois extension of $R$ with group $\Gamma$ [DI, p.84].) Since (*) is an equivalent definition of $S$ being a Galois extension of $R$ with group $\Gamma$, (*) implies that $\ell$: $S \otimes S \to C(\Gamma, S)$ is an isomorphism, and hence, (*) implies (1.1). So we show that (1.1) implies (*). Let $h$ be in $C(\Gamma, S)$ where $h(\gamma) = \delta_{\gamma,1}$. Since $\ell$: $S \otimes S \to C(\Gamma, S)$ is surjective, there are $x_1, \ldots, x_n, y_1, \ldots, y_n$ in $S$ with $h = \ell(\Sigma x_i \otimes y_i)$. Hence,

$$\begin{aligned} \delta_{\gamma,1} &= h(\gamma) \\ &= \ell\left(\sum_{i=1}^{n} x_i \otimes y_i\right)(\gamma) \\ &= \sum_{i=1}^{n} x_i \gamma(y_i) \end{aligned}$$

and (1.1) is true.

Note that if (1.1) holds, then $\ell$: $S \otimes S \to C(\Gamma, S)$ is automatically injective and hence, an isomorphism. For (1.1) is an equivalent definition for $S$ to be a Galois extension of $R$ with group $\Gamma$.

Theorem 1.2: Suppose we have a $G$-diagram of $S$ over $R$ with $S$ a strongly separable $R$-algebra. Then

(a) If $S^G$ is a separable $R^G$-algebra, then $S$ is a projective $R\cdot S^G$-module.

(b) Assume, in addition, that there is a finite group $\Gamma$ contained in the ring automorphisms of $S$ with $S^\Gamma = R$ and $(S^G)^\Gamma = R^G$. If $S^G$ is a Galois extension of $R^G$ with group $\Gamma|S^G$, then $R\cdot S^G$ is a Galois extension of $R$ with group $\Gamma|R\cdot S^G$.

Proof: (a) Since $S^G$ is a separable $R^G$-algebra, $R\otimes_{R^G}S^G$ is a separable $R^G\otimes_{R^G}R = R$ algebra [DI, 1.7, p.44].

Now

$$\mu\colon R\otimes_{R^G}S^G \to R\cdot S^G,$$

where $\mu(\Sigma r_i\otimes s_i) = \Sigma r_i s_i$ for $r_i$ in $R$ and $s_i$ in $S^G$, is a surjective ring homomorphism. Hence $R\cdot S^G$ is also a separable $R$-algebra. But $R\cdot S^G$ is a separable subextension of the strongly separable extension $S$ of $R$. Thus $S$ is a projective $R\cdot S^G$ module [DI, 2.3, p.48].

(b) Assume that $S^G$ is a Galois extension of $R^G$ with group $\Gamma|S^G$. Since $\Gamma|S^G$ is contained in the automorphisms of $S^G$, $\Gamma|R\cdot S^G$ is contained in the automorphisms of $R\cdot S^G$. And

$$R \subseteq (R\cdot S^G)^\Gamma \subseteq S^\Gamma = R.$$

So by (1.1) we need only show that

$$\ell\colon (R\cdot S^G)\otimes_R(R\cdot S^G) \to C(\Gamma|R\cdot S^G, R\cdot S^G)$$

is surjective. Since $S^G$ is a Galois extension of $R^G$ with group $\Gamma|S^G$, $R\otimes_{R^G}S^G$ is a Galois extension of $R = R\otimes_{R^G}R^G$ with group $\Gamma|R\otimes_{R^G}S^G$ where $\gamma(r\otimes s) = r\otimes\gamma(s)$ [DI, 1.3, p.85]. Hence,

$$\ell'\colon \quad (R\otimes_{R^G}S^G)\otimes_R(R\otimes_{R^G}S^G) \to C(\Gamma|R\otimes_{R^G}S^G,\ R\otimes_{R^G}S^G),$$

where

$$\begin{aligned}\ell'\colon(r_1\otimes s_1\otimes r_2\otimes s_2)(\gamma) &= (r_1\otimes s_1)\gamma(r_2\otimes s_2)\\ &= (r_1\otimes s_1)(r_2\otimes\gamma s_2)\\ &= r_1r_2\otimes s_1\gamma(s_2)\end{aligned}$$

with $r_1, r_2$ in $R$ and $s_1, s_2$ in $S^G$, is an isomorphism. Note again that $\mu\colon\ R\otimes_{R^G}S^G \to R\cdot S^G$ is a surjective ring homomorphism. Thus we have the following diagram:

$$\begin{tikzcd} R\cdot S^G\otimes_R R\cdot S^G \arrow[r, "\ell"] & C(\Gamma|R\cdot S^G, R\cdot S^G) \\ (R\otimes_{R^G}S^G)\otimes_R(R\otimes_{R^G}S^G) \arrow[u, "\mu\otimes\mu"] \arrow[r, "\ell'"] & C(\Gamma|R\otimes_{R^G}S^G, R\otimes_{R^G}S^G) \arrow[u, "\beta"'] \end{tikzcd}$$

where $\beta(f)(\gamma) = \mu(f(\gamma))$ for $f$ in $C(\Gamma|R\otimes_{R^G}S^G, R\otimes_{R^G}S^G)$.

The diagram commutes:

$$\begin{aligned}(\ell\mu\otimes\mu(r_1\otimes s_1\otimes r_2\otimes s_2))(\gamma) &= \ell(r_1s_1\otimes r_2s_2)(\gamma)\\ &= r_1s_1\gamma(r_2s_2)\\ &= r_1r_2s_1\gamma(s_2)\\ &= \mu(r_1r_2\otimes s_1\gamma(s_2))\\ &= \beta\ell'(r_1\otimes s_1\otimes r_2\otimes s_2)(\gamma)\end{aligned}$$

with $r_1, r_2$ in $R$ and $s_1, s_2$ in $S^G$. Since $\mu\otimes\mu$, $\ell'$, and $\beta$ are surjective, $\ell\colon R\cdot S^G\otimes R\cdot S^G \to C(\Gamma|R\cdot S^G, R\cdot S^G)$ is surjective. So by (1.1) $R\cdot S^G$ is a Galois extension of $R$ with group $\Gamma|R\cdot S^G$.

Theorem 1.2 implies that $R\cdot S^G$ plays an important role in $S^G$ being a separable or Galois extension of $R^G$. We shall see that this is the case later in this chapter and in the next chapter.

Suppose that we have a G-diagram of $S$ over $R$ and that $S$ is Galois extension of $R$ with group $\Gamma$ such that $(S^G)^\Gamma = R^G$. In studying to see if $S^G$ is a Galois extension of $R^G$, the following commutative diagram arises:

$$\begin{array}{ccc} S\otimes_R S & \xrightarrow{\ \ell\ } & C(\Gamma, S)\\ \uparrow{\scriptstyle\alpha} & & \uparrow{\scriptstyle j}\\ S^G\otimes_{R^G}S^G & \xrightarrow{\ \ell'\ } & C(\Gamma|S^G, S^G)\end{array}$$

where

$$\ell(s\otimes t)(\gamma) = s\gamma(t),$$

$$\ell'(a\otimes b)(\gamma) = a\gamma(b),$$

$$\alpha(a\otimes_{R^G} b) = a\otimes_R b,$$

and

$$j \text{ is the inclusion,}$$

for $s,t$ in $S$ and $a,b$ in $S^G$. Since $S$ is a Galois extension of $R$ $\ell$: $S\otimes S \to C(\Gamma,S)$ is an isomorphism. Hence, in the case that $S^G$ is a Galois extension of $R^G$ with group $\Gamma|S^G$, then $\ell'$: $S^G\otimes S^G \to C(\Gamma|S^G,S^G)$ is an isomorphism, thus, $\alpha$: $S^G\otimes S^G \to S\otimes S$ is an injection; and a necessary condition for $S^G$ to be a Galois extension of $R^G$ is the injectivity of $\alpha$.

We now show that if $S$ is a strongly separable extension of $R$, then the nilradical of $R$ lifts to the nilradical of $S$. We will need this in the next chapter.

<u>Lemma 1.3</u>: Let $S$ be a finitely generated and projective $R$-module. Then

$$(\text{nilrad}(R))S = \bigcap_{p \text{ in } \mathrm{Spec}(R)} (pS).$$

<u>Proof</u>: Clearly,

$$(\text{nilrad}(R))S = (\cap p)s \subseteq \bigcap_{p \text{ in } \mathrm{Spec}(R)} (pS).$$

So we show the opposite inclusion. Suppose that $S$ is a free R-module. Then $S = Rb_1 \oplus \ldots \oplus Rb_n$. If $x$ is in $\cap(pS)$, then $x = \Sigma r_i b_i$ with $r_i$ in $p$ for all $p$ in $\mathrm{Spec}(R)$. Hence, $r_i$ is in $\cap p$, and thus, $x$ is in $(\cap p)S = (\mathrm{nilrad}(R))S$.

If $S$ is a projective R-module, it is the direct summand of a free. So apply the free case.

Lemma 1.4: Let $S$ be a strongly separable R-algebra. If $R$ is a domain, then

$$\mathrm{nilrad}(S) = 0.$$

Proof: We have the inclusion

$$R \hookrightarrow K$$

where $K$ is the quotient field of $R$. Since $S$ is a projective R-module, $S$ is flat. So

$$S = S \otimes_R R \to S \otimes_R K$$

is an inclusion. But $S \otimes_R K$ is a strongly separable extension of $K$ since $S$ is a strongly separable R-algebra. Thus $S \otimes_R K$ is reduced, i.e., $\mathrm{nilrad}(S) = 0$ [DI, 2.4, p.49].

Theorem 1.5: Let $S$ be a strongly separable R-algebra. Then

$$\mathrm{nilrad}(S) = (\mathrm{nilrad}(R))S.$$

In particular, $\mathrm{nilrad}(S) = 0$ if and only if $\mathrm{nilrad}(R) = 0$

Proof: We always have $\mathrm{nilrad}(R)S \subseteq \mathrm{nilrad}(S)$. So we show the opposite inclusion.

Since $S$ is a strongly separable R-algebra, $S/pS$

is a strongly separable $R/p$-algebra for each $p$ in $\mathrm{Spec}(R)$ [DI, 1.7, p.44]. By (1.4) $\mathrm{nilrad}(S/pS) = 0$ for all $p$ in $\mathrm{Spec}(R)$. Thus by the Correspondence Theorem

$$\bigcap_{\substack{p \text{ in } \mathrm{Spec}(R) \\ pS \subseteq q}} q = pS .$$

Hence,

$$\mathrm{nilrad}(S) \subseteq \bigcap_{pS \subseteq q} q = \bigcap (pS) = (\mathrm{nilrad}(R))S$$

by (1.3).

Next we give sufficient criteria for $S^G$ to be a Galois extension of $R^G$. But first two lemmas:

Lemma 1.6: Let $M$ be an $R$-module and $T$ an $R$-algebra with $R \hookrightarrow T$ a split monomorphism. If $M \otimes_R T = 0$, then $M = 0$.

Proof: Since $R \hookrightarrow T$ splits,

$$M = M \otimes_R R \to M \otimes_R T$$

is a monomorphism. Thus if $M \otimes T = 0$, then $M = 0$.

Lemma 1.7: Let $A$ and $B$ be $R$-modules and $T$ an $R$-algebra with $R \hookrightarrow T$ a split monomorphism. Let $h: A \to B$ be an $R$-morphism. If $h \otimes 1: A \otimes T \to B \otimes T$ is surjective, then $h$ is surjective; if $h \otimes 1$ is injective, then $h$ is injective.

Proof: Now

$$A \xrightarrow{h} B \longrightarrow B/\mathrm{Im}h \longrightarrow 0$$

is exact. Hence,

$$A \otimes T \xrightarrow{h\otimes 1} B\otimes T \longrightarrow B/\mathrm{Im}h\otimes T \longrightarrow 0$$

is exact. But if $h\otimes 1$ is surjective, then $B/\mathrm{Im}h\otimes T = 0$. By the previous lemma $B/\mathrm{Im}h = 0$; whence, $h$ is surjective.

Assume that $h\otimes 1$: $A\otimes T \longrightarrow B\otimes T$ is injective. Then

$$\begin{aligned} h\otimes 1(\ker(h)\otimes T &= h(\ker(h))\otimes T \\ &= 0\otimes T \\ &= 0. \end{aligned}$$

Thus $\ker(h)\otimes T = 0$ since $h\otimes 1$ is injective. And by (1.6) $\ker(h) = 0$.

Theorem 1.8: Suppose that we have a G-diagram of $S$ over $R$ and $S$ is Galois extension of $R$ with group $\Gamma$ such that $(S^G)^\Gamma = R^G$. Assume that $R^G \hookrightarrow R$ is a split monomorphism. If $\mu$: $R\otimes_{R^G} S^G \to S$, where $\mu(r\otimes s) = rs$, is an isomorphism, then $S^G$ is a Galois extension of $R^G$ with group $\Gamma|S^G$.

Proof: Suppose that $\mu$: $R\otimes S^G \to S$ is an isomorphism. Since $(S^G)^\Gamma = R^G$ is given, we need only show that $\ell'$: $S^G\otimes_{R^G} S^G \to C(\Gamma|S^G, S^G)$, where $\ell'(s\otimes t)(\gamma) = s\gamma(t)$ for $s,t$ in $S^G$, is an isomorphism. We have the following commutative diagram, where $\ell$: $S\otimes_R S \to C(\Gamma,S)$ is as in (1.1), $\alpha(s\otimes t\otimes r) = (s\otimes r)\otimes(t\otimes 1)$ with $s,t$ in $S^G$ and $r$ in $R$, $(\beta(f))(\gamma) = \mu(f(\gamma))$ for $f$ in $C(\Gamma, S^G\otimes_{R^G} R)$, and

$\delta(f\otimes r)(\gamma) = f(\gamma)\otimes r$ for $r$ in $R$ and $f$ in $C(\Gamma|S^G,S^G)$:

$$\begin{tikzcd}
S\otimes_R S \arrow[r, "\ell"] & C(\Gamma,S) \\
(S^G\otimes_{R^G}R)\otimes_R(S^G\otimes_{R^G}R) \arrow[u, "\mu\otimes\mu"'] & C(\Gamma,S^G\otimes_{R^G}R) \arrow[u, "\beta"'] \\
S^G\otimes_{R^G}S^G\otimes_{R^G}\otimes^R \arrow[u, "\alpha"'] \arrow[r, "\ell'\otimes\ell"] & C(\Gamma|S^G,S^G)\otimes_{R^G}R \arrow[u, "\delta"']
\end{tikzcd}$$

The diagram does indeed commute:

$$\begin{aligned}
(\ell(\mu\otimes\mu)\alpha)(s\otimes t\otimes r)(\gamma) &= \ell(\mu\otimes\mu)((s\otimes r)\otimes(t\otimes 1))(\gamma) \\
&= \ell(sr\otimes t)(\gamma) \\
&= sr\gamma(t) \\
&= \mu(s\gamma(t)\otimes(\gamma)) \\
&= \beta\delta(\ell' s\otimes t)\otimes r)(\gamma) \\
&= \beta\delta(\ell'\otimes 1)(s\otimes t\otimes r)(\gamma)
\end{aligned}$$

for $s,t$ in $S^G, r$ in $R^G$, and $\gamma$ in $\Gamma$. Clearly, $\mu\otimes\mu, \alpha$, and $\beta$ are $R^G$-isomorphisms. Since $S$ is a Galois extension of $R$ with group $\Gamma$, $\ell$ is an isomorphism. And on page 20 of [M], we see that $\delta$ is an $R^G$-isomorphism. Hence, with the diagram commutative and all the maps isomorphisms, we have that $\ell'\otimes 1$ is an isomorphism. By (1.7) $\ell'$ is an isomorphism.

(1.9) together with the proof of (1.2) says that if $R^G \hookrightarrow S^G$ is a split monomorphism (a necessary condition), then $S^G$ is a Galois extension of $R^G$ with group $\Gamma|S^G$

if and only if $R\otimes_{R^G}S^G$ is a Galois extension of $R$ with group $\Gamma$.

Remark 1.10: Suppose that $S \supseteq T \supseteq R$ where $S$ and $T$ are Galois extensions of $R$ with the same group $\Gamma$, i.e., $\gamma_1|T \neq \gamma_2|T$ for any $\gamma_1,\gamma_2$ in $\Gamma$. Then $S = T$.

Proof: If $R$ is an algebraically closed field, then since the $\dim_R(S)$ and $\dim_R(T)$ is the order of $\Gamma$, $S = \overset{n}{\underset{i=1}{\times}} R = T$ where $n$ is the order of $\Gamma$ [DI, 1.3(4),P.85]. Now suppose $R$ is a field and $F$ is the algebraic closure of $R$. Then $T\otimes_R F$ and $S\otimes_R F$ are both Galois extensions of $F = R\otimes_R F$ with group $\Gamma$ [DI, 1.3(3), P.85]. And hence, $T\otimes_R F = S\otimes_R F$. But then $\dim_R T = \dim_F(T\otimes_R F) = \dim_F(S\otimes_R F) = \dim_R S$, and $T = S$. In general, we get $S$ a strongly separable $T$-algebra [DI, 2.4, P.94], and $S = T\oplus M$ where $M$ is a finite $T$-module [DI, 4.2, P.56]. But $S/mS = T/mS$ for all $m$ in $\mathrm{Max}(R)$ by the above. Thus $M/mM = 0$ for all $m$ in $\mathrm{Max}(R)$. In particular, $M = 0$ and $T = S$.

Corollary 1.11: Suppose that we have a $G$-diagram of $S$ over $R$ with $S$ Galois extension of $R$ with group $\Gamma$ where $(S^G)^\Gamma = R^G$. If $\Gamma|S^G = \Gamma$, and $S^G$ is a Galois extension of $R^G$ with group $\Gamma$, then $S$ is invariantly generated over $R$, i.e., $S = R\cdot S^G$.

Proof: By (1.2) we have that $R\cdot S^G$ is a Galois extension of $R$ with group $\Gamma|R\cdot S^G$.

Since $\Gamma | S^G = \Gamma$, $\Gamma | R \cdot S^G = \Gamma$. Hence, we have $R \cdot S^G$ contained in $S$ and both Galois extensions of $R$ with the same group. Therefore, $S = R \cdot S^G$ by the previous remark.

The next two theorems treat the problem when $G$ is a finite group.

<u>Theorem 1.12</u>: Suppose that we have a $G$-diagram of $S$ over $R$ where $S$ is a strongly separable $R$-algebra. If $G$ is finite and $R = R^G$, then $S^G$ is a strongly separable $R = R^G$-algebra.

<u>Proof</u>: Since $S$ is a separable $R$-algebra and $R = R^G \subseteq S^G \subseteq S$, $S$ is a separable extension of $S^G$. Hence, with $G$ finite $S$ is a strongly separable $S^G$-algebra [K]. Thus $S^G$ is a strongly separable $R^G$-algebra [DI, 2.4, P.94].

<u>Corollary 1.13</u>: Suppose that we have a $G$-diagram of $S$ over $R$ where $S$ is strongly separable $R$-algebra. If $S$ has no idempotents but $0,1$ and $R = R^G$, then $S^G$ is a strongly separable $R^G$-algebra.

Proof: Since $S$ is a finite $R$-module and a separable $R$-algebra, $S$ is a finite $S^G$-module and separable $S^G$-algebra $(R = R^G \subseteq S^G \subseteq S)$. Thus with $S$ having no nontrivial idempotents, $G$ is finite [N, Theorem 1]. Now apply (1.12).

For the remainder of this chapter we will treat the problem when $R$ is a finite product of fields. In this case we replace the strongly separable question with a weakly Galois question: If $S$ is a weakly Galois extension of $R$ with finite group $\Gamma$ and $(S^G)^\Gamma = R^G$, is $S^G$ a weakly Galois extension of $R^G$ with group $\Gamma|S^G$? We find via the next two lemmas that this is the case.

Lemma 1.14: Let $S$ be a finite product of fields and $G$ contained in the ring automorphisms of $S$. Then $S^G$ is a finite product of fields.

Proof: Now $S = Se_1 \times \ldots \times Se_n$ where the $e_i$ are minimal idempotents and the $Se_i$ are fields. Let $S^G = S^G f_1 \times \ldots \times S^G f_k$ be a decomposition of $S^G$ with the $f_i$ minimal idempotents of $S^G$. Let $f = f_i$ for any $i = 1, \ldots, k$ and consider $Sf$. Now $Sf = Se_{i_1} \times \ldots \times Se_{i_m}$ where the $e_{i_j}$ are among $e_1, \ldots, e_n$ and $f = e_{i_1} + \ldots + e_{i_m}$.

Let $s$ be in $S^G$ with $sf \neq 0$. Then

$sf = se_{i_1} + \ldots + se_{i_m}$. Note that for $j = 1, \ldots, m$,

$se_{i_j} \neq 0$. For suppose for some $j$'s that $se_{i_j} = 0$.

Then $sf = se_{l_1} + \ldots + se_{l_t}$ where $e_{l_i}$ are in

$\{e_{i_1}, \ldots, e_{i_m} | se_{i_j} \neq 0\}$, and this is unique representation

by direct sum. But $\Sigma_{i=1}^{t} e_{1_i}$ is not in $S^G$ or else $f$ would not be a minimal idempotent of $S^G$. Also, for all $\sigma$ in $G$, $\sigma(e_{1_i})$ is in $\{e_{i_1}, \ldots, e_{i_m}\}$:
$e_{i_1} + \ldots + e_{i_m} = f = \sigma(f) = \sigma(e_{i_1}) + \ldots + \sigma(e_{i_m})$ and $\sigma(e_{i_j})$ minimal idempotents imply by uniqueness of direct sum that $\sigma(e_{i_j})$ is among $e_{i_1}, \ldots, e_{i_m}$. Thus, for $\sigma$ in $G$ with

$$\sigma(\Sigma_{i=1}^{t} e_{1_i}) \neq \Sigma_{i=1}^{t} e_{1_i} ,$$

$$sf = \sigma(sf) = \sigma(s\Sigma_{i=1}^{t} e_{1_i}) = s\Sigma_{i=1}^{t}(e_{1_i})$$

is a second unique representation of $sf$ which is a contradiction.

Since $se_{i_j} \neq 0$ for $j = 1, \ldots, m$, there is for each $j$ an $s_j$ in $S$ with $se_{i_j} s_j e_{i_j} = e_{i_j}$ in the field $Se_{i_j}$. So if $t = s_1 e_{i_1} + \ldots + s_m e_{i_m}$, then $sft = f$. Note that $tf = t$ since $t$ is in $Sf$, and hence, $st = stf = f$. Let $\sigma$ be in $G$. We snow that $t$ is in $S^G$. Then $s\sigma(t) = \sigma(st) = \sigma(f) = f = st$. Thus we get the following:

$$s\sigma(t) = st$$

$$ts\sigma(t) = tst$$

$$f\sigma(t) = ft$$

$$\sigma(ft) = t$$

$$\sigma(t) = t.$$

This is true for all $\sigma$ in $G$, whence $t$ is in $S^G$. And $t = tf$ is an element of $S^G f$ such that $t(sf) = f$, the identity in $S^G f$, i.e., $S^G f$ is a field.

<u>Lemma 1.15</u>: Let $S = Se_1 \times \ldots \times Se_n$ be a finite product of fields and $\Gamma$ a group of automorphisms of $S$ which is finite. Then $S$ is a strongly separable $S^\Gamma$-algebra.

<u>Proof</u>: (The first paragraph comes from [I, 2.15].)

Let $He_i = \{\sigma \text{ in } \Gamma \mid \sigma(e_i) = e_i\}$. Note that $He_i$ is a finite group of $S^\Gamma e_i$ automorphisms of $Se_i$. Also, $\Gamma = \sigma_1 He_i \cup \ldots \cup \sigma_n He_i$ (disjoint union with $\sigma_1$ equal to the identity). Thus if $i \neq 1$, $\sigma_i(e_i)e_i = 0$. Let $se_i$ be in $(se_i)^{He_i}$. Then

$$\sum_{j=1}^{n} \sigma_j(se_i)e_i = \sum_{j=1}^{n} \sigma_j(s)\sigma_j(e_i)e_i = se_i .$$

But $\sum_{j=1}^{n} \sigma_j(se_i)$ is in $S^\Gamma$; for $\sigma_j = \sigma_k \bar{\sigma}_k$ where $\bar{\sigma}_k$ is in $He_i$ implies that $\sigma_j(se_i) = \sigma_k\bar{\sigma}_k(se_i) = \sigma_k(se_i)$ since $se_i$ is in $(Se_i)^{He_i}$. Thus $se_i$ is in $S^\Gamma e_i$, and hence, $(Se_i)^{He_i} = S^\Gamma e_i$.

Since $Se_i$ is a field and $(Se_i)^{He_i} = S^\Gamma e_i$, $Se_i$ is a Galois extension of $S^\Gamma e_i$ with group $He_i$, and hence, $Se_i$ is a separable $S^\Gamma e_i$-algebra. From the proof of (1.14), $S^\Gamma = S^\Gamma f_1 \times \ldots \times S^\Gamma f_t$ where the $f_i$ are minimal idempotents of $S^\Gamma$ and $f_i = e_{i_1} + \ldots + e_{i_k}$ with the $e_{i_j}$

among $e_t$ for $t = 1, \ldots, n$. Note that for all $j$, $f_i e_{i_j} = e_{i_j}$. Thus $S^\Gamma F_i \cong S^\Gamma f_i e_{i_j} = S^\Gamma e_{i_j}$ for all $j$. Hence, $Se_{i_j}$ is a separable $S^\Gamma f_i$-algebra for all $j$; whence $Se_{i_1} \times \ldots \times Se_{i_k}$ is a separable $S^\Gamma f_i$-algebra since it is a finite product of separable field extensions of $S^\Gamma f_i$ [DI, 2.4, P.49]. Thus $S = \times_{i=1}^{t} (Se_{i_1} \times \ldots \times Se_{i_k})$ is a separable $S^\Gamma = S^\Gamma f_1 \times \ldots \times S^\Gamma f_t$-algebra since we have a ring direct sum and $Se_{i_1} \times \ldots \times Se_{i_k}$ is a separable $S^\Gamma f_i$-algebra for each $i = 1, \ldots, t$ [DI, 1.13, P. 47]. Since $\Gamma$ is finite and $S$ is a separable $S^\Gamma$-algebra, $S$ is a strongly separable $S^\Gamma$-algebra [K].

<u>Theorem 1.16</u>: Suppose that we have a $G$-diagram of $S$ over $R$ and $S$ is a weakly Galois extension of $R$ with group $\Gamma$ such that $(S^G)^\Gamma = R^G$. If $R$ is a finite product of fields, then $S^G$ is a weakly Galois extension of $R^G$ with group $\Gamma|S^G$.

<u>Proof</u>: Since $S$ is a strongly separable $R$-algebra, $JRad(S) = JRad(R)S$ [I, 1.1]. Hence, $JRad(S) = 0$ since $JRad(R) = nilrad(R) = 0$. Also, $S$ is finitely generated as a module over the artinian ring $R$, and hence, $S$ is artinian. Since also $JRad(S) = 0$, $S$ is a finite product of fields. By (1.14) $S^G$ is a finite product of fields. Since $(S^G)^\Gamma = R^G$ and $\Gamma$ is finite, we apply (1.15) to

get that $S^G$ is a strongly separable $R^G$-algebra.

<u>Corollary 1.17</u>: Suppose that we have a G-diagram of S over R and S is a weakly Galois extension of R with group $\Gamma$ such that $g\gamma = \gamma g$ for all $\gamma$ in $\Gamma$ and g in G. If R is a finite product of fields, then $S^G$ is a weakly Galois extension of $R^G$ with group $\Gamma|S^G$.

<u>Proof</u>: If $\Gamma|S^G$ is contained in the automorphisms of $S^G$ and $(S^G)^\Gamma = R^G$, then the corrollary will follow from the previous theorem.

a. $(\ )|: \to \mathrm{Aut}_{R^G}(S^G)$ by $(\gamma)| = \gamma|S^G$ is well-defined:

i. Let s be in $S^G$ and $\gamma$ in $\Gamma$. Then for each g in G, $g(s) = s$ implies that $g(\gamma(s)) = \gamma(g(s)) = \gamma(s)$. Hence, $\gamma(s)$ is in $S^G$.

ii. Let s be in $S^G$ and $\gamma$ in $\Gamma$. There is an s' in S with $\gamma(s') = s$. For each g in G, $\gamma g(s') = g\gamma(s') = g(s) = s$. But $\gamma(s') = s = \gamma(g(s'))$ implies that $s' = g(s')$. Thus s' is in $S^G$.

iii. Let $\gamma$ be in $\Gamma$ and r in $R^G$. Then r is in $R = S^\Gamma$; whence, $\gamma(r) = r$. Let s be in $S^G$ with $\gamma(s) = s$ for $\gamma$ in $\Gamma$. Then s is in $S \cap S^G = R \cap S^G = R^G$.

b. $(S^G)^\Gamma = R^G$:

i. Let r be in $R^G$, i.e., $g(r) = r$ for all g in G. Then $\gamma g(r) = \gamma(r) = r$ for all $\gamma$ in $\Gamma$ and g in G. Thus r is in $(S^G)^\Gamma$.

ii. Let $s$ be in $(S^G)^\Gamma$. Then $\gamma g(s) = s$ for all $\gamma$ in $\Gamma$ and $g$ in $G$. Now $S^G$ a subset of $S$ implies that $(S^G)^\Gamma \subseteq S^\Gamma = R$, i.e., $s$ is in $R$. But $s$ is also in $S^G$. So $s$ is in $R \cap S^G = R^G$.

Note that (1.17) shows that if we have a G-diagram of $S$ over $R$ and a group $\Gamma$ entirely unrelated to $G$, then $\Gamma|S^G$ is contained in the automorphisms of $S^G$ and $(S^G)^\Gamma = R^G$.

<u>Corollary 1.18</u>: Suppose that we have a G-diagram of $S$ over $R$ with $S$ a weakly Galois extension of $R$ with group $\Gamma$ and $(S^G)^\Gamma = R^G$. If $R$ is reduced, $S^G$ is a finite $R^G$-module, and $R^G$ is artinian, then $S^G$ is a weakly Galois extension of $R^G$ with group $\Gamma|S^G$.

<u>Proof</u>: By (1.5) $S$ is reduced, and hence $S^G$ has no non-zero nilpotents. Since $S^G$ is finitely generated as a module over the artinian ring $R^G$, $S^G$ is a finite product of fields. By (1.15) $S^G$ is a strongly separable $R^G$-algebra.

Now (1.15) shows that if $S$ is a finite product of fields and $\Gamma$ is a finite group of automorphisms of $S$, then $S$ is a strongly separable $S^\Gamma$-algebra. Without anymore hypothesis this is the most we can say, i.e., $S$ does not have to be a Galois extension of $S^\Gamma$ with group $\Gamma$. So Artin's Theorem [L, 2, P.194], which says that if $S$

is a field and $\Gamma$ a finite group of ring automorphisms of $S$, then $S$ is a Galois extension of $S^{\Gamma}$, does not extend to the case in which $S$ is a finite product of fields as the following example shows:

(1.19) Let $S = Q\times Q\times Q$ and $\Gamma = \{\sigma_1, \sigma_2\}$ where $\sigma_1$ is the identity and $\sigma_2(a,b,c) = (b,a,c)$. Let $M = Q\times Q\times\{0\}$, a maximal ideal of $S$. Then

$$\begin{aligned}\sigma_2(a,b,c) - (a,b,c) &= (b,a,c) - (a,b,c)\\ &= (b - a,\ a - b,\ 0)\end{aligned}$$

which is in $M$. Thus there does not exist any $s$ in $S$ with $\sigma_2(s) - s$ not in $M$. Hence $S$ is not a Galois extension of $S^{\Gamma}$ [DI, 1.2(5), P.81].

We now study the question of $S^G$ being a Galois extension of $R^G$. We find necessary and sufficient conditions for $S^G$ to be a Galois extension of $R^G$ when $R$ is a finite product of fields and then give two examples that show that $S$ being a Galois extension of $R$ has no bearing on the question. But first a technical lemma.

<u>Lemma 1.20</u>: Let $S = Se_1\times \ldots \times Se_n$ be a finite product of fields and $G$ be a finite group of automorphisms of $S$. Then $S$ is a Galois extension of $S^G$ if and only if for each $\sigma \neq$ identity in $G$, $\sigma|Se_i\colon Se_i \to S$ is not the identity for any $i$.

<u>Proof</u>: Suppose that for all $\sigma \neq$ identity in $G$ $\sigma|Se_i\colon Se_i \to S$ is not the identity. Note that if $M$ is

a maximal ideal in $S$, then $M = Se_{j_1} \times \ldots \times Se_{j_{n-1}}$, i.e., $M$ is a subproduct of $n-1$ factors of $S$. This follows since $M = MSe_1 \times \ldots \times MSe_n$ and if $M = Se_{j_1} \times \ldots \times Se_{j_k}$ with $k < n-1$, then $M$ is not maximal. For convenience assume that $M = Se_1 \times \ldots \times Se_{n-1}$. Let $\sigma \neq$ identity be in $G$.

Case 1: Suppose that $\sigma(e_n) = e_n$. Let $s$ be in $S$ with $\sigma(se_n) \neq se_n$. Then $\sigma(se_n) - se_n \neq 0$; whence, $\sigma(se_n) - se_n$ is not in $M$.

Case 2: Suppose that $\sigma(e_n) \neq e_n$. Then $\sigma(e_n) - e_n \neq 0$; and hence, $\sigma(e_n) - e_n$ is not in $M$.

Conversely, suppose that $S$ is a Galois extension of $S^G$ with group $G$. Also, assume that there is a $\sigma \neq$ identity in $G$ with $\sigma|Se_i =$ identity on $Se_i$ for some $i$. Let $M = Se_1 \times \ldots \times Se_{i-1} \times Se_{i+1} \times \ldots \times Se_n$, a maximal ideal of $S$. Let $s$ be in $S$. Then $s = se_1 + \ldots + se_n$ and

$$\sigma(s) - s = \sum_{j \neq i} \sigma(se_j) + se_i - \Sigma se_j = \sum_{j \neq i} (\sigma(s) - s)e_j$$

since $\sigma$ permutes the $e_j$. Thus $\sigma(s) - s$ is in $M$ for all $s$ in $S$. Hence, $S$ is not a Galois extension of $S^G$, a contradiction.

Theorem 1.21: Suppose that we have a $G$-diagram of $S$ over $R$ and a finite group $\Gamma$ contained in the automorphisms of $S$ such that $S^\Gamma = R$ and $(S^G)^\Gamma = R^G$. Also, assume that $R$ is a finite product of fields. Then $S^G$ is a

Galois extension of $R^G$ with group $\Gamma|S^G$ if and only if $R\cdot S^G$ is a Galois extension of $R$ with group $\Gamma|R\cdot S^G$.

Proof: By (1.15) $S$ is a weakly Galois extension of $R$ with group $\Gamma$. And then by (1.15) $S^G$ is a weakly Galois extension of $R^G$ with group $\Gamma|S^G$. Applying (1.2) we find that $R\cdot S^G$ is a strongly separable $R$-algebra, and since $R \subseteq (R\cdot S^G)^\Gamma \subseteq S^\Gamma = R$, $(R\cdot S^G)^\Gamma = R$. We noted in the proof of (1.16) that a strongly separable extension of a finite product of fields is a finite product of fields. Hence, $R\cdot S^G$ is a finite product of fields.

Since $R\cdot S^G$ and $S^G$ are finite products of fields, $R\cdot S^G = R\cdot S^G e_1 \times \ldots \times R\cdot S^G e_n$ and $S^G = S^G f_1 \times \ldots \times S^G f_t$ for $e_i$ and $f_i$ minimal idempotents in $R\cdot S^G$ and $S^G$ respectively. Suppose that $R\cdot S^G$ is a Galois extension of $R$ with group $\Gamma|R\cdot S^G$. For $S^G$ to be a Galois extension of $R^G$, we need that if $\gamma|S^G$ is not the identity, then $\gamma|S^G f_I \neq$ identity for all $i$. Let $f = f_i$ for any $i = 1, \ldots, t$. Now $f = e_{i_1} + \ldots + e_{i_k}$ for $e_{i_j}$ among $e_1, \ldots, e_n$. Assume that $\gamma|S^G f =$ identity. Then $\gamma(f) = f$, and hence, $\gamma$ permutes the $e_{i_j}$. Suppose that for some $e = e_{i_j}$, $\gamma(se) = se$ for all $s$ in $S^G$. Note that $\gamma(e) = e$. So $\gamma(\Sigma r_i s_i e) = \Sigma r_i s_i e$ for $r_i$ in $R$ and $s_i$ in $S^G$. Since $R\cdot S^G$ is a Galois extension of $R$, $\gamma|R\cdot S^G e =$ identity if and only if $\gamma =$ identity. Hence, in this case there is a $s$ in $S^G$ with $\gamma(s)e = \gamma(se) \neq se$. Thus $\gamma(sf) = \gamma(se_{i_1}) + \ldots + \gamma(se_{i_k}) \neq se_{i_1} + \ldots + se_{i_k} = sf$, and $S^G f$ cannot be the identity. Now assume that $\gamma$ does not fix any of the $e_{i_j}$ for $j = 1, \ldots, k$ and that for $e = e_{i_j}$, $\gamma(e) = e'$ where $e' = e_{i_j}$ for some $j \neq 1$. If $\gamma(se) = se'$ for every $s$ in $S^G$, then $\gamma((\Sigma r_i s_i)e) = \Sigma r_i s_i e'$ for $r$ in $R$ and $s$ in $S^G$. This means that $\gamma(te) = te'$ for every $t$ in $R\cdot S^G$. In particular,

$$e' = \gamma(e) = \gamma(ee) = ee' = 0,$$

which is absurd. So there is a $s$ in $S^G$ with $\gamma(s)e' = \gamma(se) \neq se'$, and $\gamma|S^G f$ cannot be the identity. Therefore, in all cases if $\gamma|S^G$ is not the identity, then $\gamma|S^G f$ is not the identity, and $S^G$ is a Galois extension of $R^G$ with group $\gamma|S^G$. The converse follows from (1.2).

The following example shows that $S^G$ may be a Galois extension of $R^G$ with group $\Gamma|S^G$ even if $S$ is not a Galois extension of $R$ with group $\Gamma$.

(1.22) Let

$$S = \mathbb{C}\times\mathbb{C}\times\mathbb{C},$$

$$R = \{(c,c,a) | c,a \in \mathbb{C}\} \cong \mathbb{C}\times\mathbb{C},$$

$$\Gamma = \{\gamma_1,\gamma_2 \quad \text{where } \gamma_1 = \text{identity and}$$

$$\gamma_2(a,b,c) = (b,a,c),$$

and

$$G = \{\sigma_1, \sigma_2\} \text{ where } \sigma_1 = \text{identity and}$$
$$\sigma_2(a,b,c) = (a,c,b).$$

Then $S^G = \{(a,c,c) \mid a,c \in \mathbb{C}\} \cong \mathbb{C}\times\mathbb{C}$, $R^G = \{(c,c,c) \mid c \in \mathbb{C}\} \cong \mathbb{C}$, and $(S^G)^\Gamma = \{(c,c,c) \mid c \in \mathbb{C}\} = R^G$, where we let $\Gamma$ act on $S^G$ by $\gamma_2(a,c,c) = (c,a,a)$. Note that $\Gamma$ is a group of automorphisms of $S^G$. By (1.20) $S^G$ is a Galois extension of $R^G$ with group $\Gamma|S^G$ and $S$ is not a Galois extension of $R$ with group $\Gamma$.

The next example shows that $S^G$ may not be a Galois extension of $R^G$ with group $\Gamma|S^G$ even if $S$ is a Galois extension of $R$ with group $\Gamma$.

(1.23) Let

$$S = \mathbb{C}\times\mathbb{C}\times\mathbb{C},$$
$$R = \{(c,c,r) \mid c \in \mathbb{C},\ r \in \mathbb{R}\} \cong \mathbb{C}\times\mathbb{R},$$
$$\Gamma = \{\gamma_1, \gamma_2\} \text{ where } \gamma_1 = \text{identity and}$$
$$\gamma_2(a,b,c) = (b,a,c),$$

and

$$G = \{\sigma_1, \ldots, \sigma_8\} \text{ where } \sigma_1 = \text{identity},$$
$$\sigma_2(a,b,c) = (\bar{a},b,c),\ \sigma_3(a,b,c) = (a,\bar{b},c),$$
$$\sigma_4(a,b,c) = (a,b,\bar{c}),\ \sigma_5(a,b,c) = (\bar{a},\bar{b},c),$$
$$\sigma_6(a,b,c) = (\bar{a},b,\bar{c}),\ \sigma_7(a,b,c) = (a,\bar{b},\bar{c}),$$
$$\sigma_8(a,b,c) = (\bar{a},\bar{b},\bar{c})$$

where $\bar{a}$ is the complex conjugate of $a$. Then

$S^G = \mathbf{R}\times\mathbf{R}\times\mathbf{R}$, $R^G = \{(c,c,r) \mid c\in\mathbb{C},\ r\in\mathbf{R}\} \cong \mathbf{R}\times\mathbf{R}$, and $(S^G)^\Gamma = \{(c,c,r) \mid c\in\mathbb{C},\ r\in\mathbf{R}\} = R^G \cong \mathbf{R}\times\mathbf{R}$. Note that $\Gamma$ is a group of automorphisms of $S^G$ and that $\gamma_2$ restricted to any of the factors of $\mathbb{C}\times\mathbb{C}\times\mathbb{C}$ is not the identity. Thus by (1.20) $S$ is a Galois extension of $R$ with group $\Gamma$. But $\gamma_2 | \{0\}\times\{0\}\times\mathbf{R}$ is the identity. So by (1.20) $S^G$ is not a Galois extension of $R^G$ with group $\Gamma | S^G$.

We end this chapter with two cases in which we get $S^G$ a strongly separable $R^G$-algebra without having to employ a finite group $\Gamma$ of automorphisms of $S^G$ with $(S^G)^\Gamma = R^G$.

<u>Theorem 1.24</u>: Suppose that we have a G-diagram of $S$ over $R$ where $S$ is a strongly separable $R$-algebra and $R$ is a finite product of fields. If $G$ is finite, then $S^G$ is a strongly separable $R^G$-algebra.

<u>Proof</u>: Since $G$ is finite, we apply (1.15) to find that $R$ is a strongly separable $R^G$-algebra. Hence, $S$ is a strongly separable $R^G$-algebra [DI, 1.12, P.46]. Since $R^G \subseteq S^G \subseteq S$ and $S$ is a separable $R^G$-algebra, $S$ is a separable $S^G$-algebra [DI, 1.2, P.46]. Since $G$ is finite and $S$ is separable $S^G$-algebra, $S$ is a projective $S^G$-module [K]. Hence, $S^G$ is a strongly separable $R^G$-algebra [DI, 2.4, P.94].

<u>Theorem 1.25</u>: Suppose that we have a G-diagram of $S$ over

$R$ where $S$ is a strongly separable extension of $R$ and $R$ is a field. If $R^G$ is algebraically closed, then $S^G$ is a strongly separable $R^G$-algebra.

Proof: Since $S$ is a finitely generated vector space over $R$, $R\cdot S^G$ is a finite dimensional $R$-vector space. We may assume that a basis for $R\cdot S^G$ over $R$ consists of elements from $S^G$, say, $\{x_1, \ldots, x_n\}$. We show that $\{x_1, \ldots, x_n\}$ generates $S^G$ as an $R^G$-module. To do this let $\sigma$ be in $G$ and suppose that

$$\Sigma\sigma(r_i)x_i = \sigma(\Sigma r_i x_i) = \Sigma r_i x_i.$$

Then,

$$\Sigma(\sigma(r_i) - r_i)x_i = 0.$$

Hence, $\sigma(r_i) - r_i = 0$ for each $i = 1, \ldots, n$ since $\{x_1, \ldots, x_n\}$ forms an $R$-basis. So if $\Sigma r_i x_i$ is in $S^G$, then the $r_i$ are in $R^G$. Thus $S^G$ is a finitely generated $R^G$-vector space. Since $S$ is strongly separable over the field $R$, $S$ is a finite product of fields. By (1.14) $S^G$ is a finite product of fields. But since $S^G$ is a finite $R^G$-module where $R^G$ is algebraically closed, $S^G = R^G \times \ldots \times R^G$; and hence, $S^G$ is a strongly separable $R^G$-algebra.

## CHAPTER II

## REDUCTIVE CASE

Throughout this chapter $G$ is a linear reductive algebraic group over $k$, where $k$ is an algebraically closed field.

Our setting is the following: we have a $G$-diagram of $S$ over $R$ where $S$ and $R$ are finitely generated $k$-algebras with $G$ acting rationally on $S$ and hence also on $R$. This will be called the Reductive Case. We find that if $S$ is a strongly separable $R$-algebra, then $S^G$ is a strongly separable $R^G$-algebra if and only if $S$ is a projective $R \cdot S^G$-module. If $S$ is a Galois extension of $R$ with group $\Gamma$, we see that $S^G$ is a Galois extension of $R^G$ if and only if $R \cdot S^G$ is a Galois extension of $R$. We then end the chapter with an example in which $S$ is a Galois extension of $R$, yet $S^G$ is not a separable $R^G$-algebra.

We now list some definitions and results from Fogarty's Invariant Theory [F].

(2.1) If $M$ is a rational $G$-module, then

$M^G = \{m$ in $M | \sigma(m) = m$ for all $\sigma$ in $G\}$ is called the <u>G-invariant</u> <u>submodule</u> of $M$.

(2.2) A rational $G$-module $M$ is called <u>G-ergodic</u> if $M^G = (0)$.

(2.3) Any rational $G$-module $M$ contains a unique maximal $G$-ergodic submodule $M_G$. Moreover, $M = M^G \oplus M_G$ and $M_G$ is the unique $G$-complement of $M^G$ in $M$.

<u>Proof</u>: [F, 5.2, P.155].

(2.4) Let $M$ be a rational $G$-module. By (2.3) there is a projection from $M = M^G \oplus M_G$ to $M^G$ whose kernel is $M_G$. This projection is denoted $P_M$ and is called the <u>Reynold's</u> <u>operator</u> of $M$.

(2.5) Let $R$ be a finitely generated $k$-algebra with $G$ acting rationally on $R$. Then $R^G$ is a finitely generated $k$-algebra.

<u>Proof</u>: [F, 5.9, P.160].

<u>Definition 2.6</u>: Let $M$ be a rational $G$-module and an $R^G$-module. Call $M$ a <u>compatible</u> $G$ and $R^G$-module if $g(rm) = g(r)g(m)$ for $g$ in $G$, $r$ in $R$, and $m$ in $M$.

The next two lemmas show that if $M$ is a compatible $G$ and $R^G$-module, then $M^G$ and $M_G$ are not only $G$-modules but also $R^G$-modules. And in the setting of this chapter, we will deal with compatible $G$ and $R^G$-modules. The first lemma is an extension of Lemma 5.4 of Fogarty's [F, 5.4, P.156].

Lemma 2.7: Let $G$ be linearly reductive and $M$ a compatible $G$ and $R^G$-module. If $r$ is in $R^G$ and $m$ in $M$, then

$$P_M(rm) = rP_M(m)$$

where $P_M$ is the Reynold's operator of $M$. In particular, $P_M$ is an $R^G$-module morphism.

Proof: Now

$$\begin{aligned} P_M(r(m - P_M(m))) &= P_M(rm) - P_M(rP_M(m)) \\ &= P_M(rm) - rP_M(m), \end{aligned}$$

since by the compatibility of the $G$ and $R^G$-module structure of $M$ if $r$ is in $R^G$, then $rP_M(m)$ is in $M^G$. Thus we reduce to showing that $P_M(r(m - P_M(m))) = 0$.

Note that $m - P_M(m)$ is in $M_G$. So we show that if $n$ is in $M_G$, then $P_M(rn) = 0$. Now $M_G = \cup N_i$ where the $N_i$ are simple G-ergodic submodules of $M$, i.e., if $n$ is in $M_G$, then $n = \Sigma n_i$ with $n_i$ in $N_i$. Thus

$$P_M(rn) = P_M(\Sigma rn_i) = \Sigma P_M(rn_i).$$

Hence, we may assume that $n$ is $N$ where $N$ is a simple G-ergodic module. Define

$$\theta: \; N \to rN \;\text{ by }\; \theta(x) = rx.$$

Clearly, $\theta$ is an $R^G$-morphism; and since

$$\theta(g(x)) = rg(x) = g(r)g(x) = g(rx) = g\theta(x)$$

for all $g$ in $G$, $\theta$ is also a G-morphism. Thus $rN$ is a G-module. But since $N$ is simple, either $rN \cong (0)$ or $N \cong rN$. But since $N$ is G-ergodic, if $N \cong rN$, then $rN$ is G-ergodic. In either case, $rN$ is contained in $M_G$, i.e., $rn$ is in $M_G$. Thus $P_M(rn) = 0$.

Corollary 2.8: Let $G$ be linearly reductive and $M$ a compatible $G$ and $R^G$-module. Then $M^G$ and $M_G$ are both $R^G$-modules.

Proof: By (2.7) $P_M: M \to M^G$ is an $R^G$-module morphism. Now $M^G$ is the image of $P_M$ and $M_G$ the kernel of $P_M$. Hence, $M^G$ and $M_G$ are $R^G$-modules.

We use the next lemma in the following theorem, which gives conditions for $S^G$ to be a finite and projective $R^G$-module.

Lemma 2.9: Let $G$ be linearly reductive and $M$ and $N$ G-ergodic modules. Then $M \oplus N$ is G-ergodic where $g(m + n) = g(m) + g(n)$ for $m$ in $M$, $n$ in $N$, and $g$ in $G$.

Proof: Suppose that $m + n$ is in $(M \oplus N)^G$. Then $m + n = g(m) + g(n)$ for all $g$ in $G$. By the G-module structure of $M$ and $N$ and direct sum,

$$m = g(m) \quad \text{and} \quad n = g(n)$$

for all $g$ in $G$. This means that $m$ is in $M^G = (0)$ and $n$ is in $N^G = (0)$, i.e., $m + n = 0$.

Theorem 2.10: Suppose that we have a G-diagram of $S$ over $R$ as in the Reductive Case.

a. If there is a finite group $\Gamma$ contained in the automorphisms of $S^G$ with $(S^G)^\Gamma = R^G$, then $S^G$ is a finite $R^G$-module.

b. If $R \cdot S^G$ is a finite $R$-module, then $S^G$ is a finite $R^G$-module.

c. If $R \cdot S^G$ is a finite and projective $R$-module, then $S^G$ is a finite and projective $R^G$-module.

d. Suppose in addition that $S$ is a strongly separable $R$-algebra. If $S^G$ is a separable $R^G$-algebra, then $S^G$ is a strongly separable $R^G$-algebra.

Proof: (a) Since $S$ is a finitely generated $k$-algebra, we apply (2.5) to find that $S^G$ is a finitely generated $k$-algebra. And hence, $S^G$ is a finitely generated $R^G$-algebra. Since $\Gamma$ is finite and $(S^G)^\Gamma = R^G$, $S^G$ is integral over $R^G$. But $S^G$ being integral and finitely generated over $R^G$ implies that $S^G$ is a finite $R^G$-module.

(b) Since $R \cdot S^G$ is a finite $R$-module, $R \cdot S^G = \Sigma_{i=1}^n Rx_i$ where we may assume that the $x_i$ are in

$S^G$. Let $s$ be in $S^G$. Then

$$\begin{aligned} s &= \Sigma r_i x_i \\ &= \Sigma r_i' x_i + \Sigma r_i'' x_i \\ &= \Sigma r_i' x_i, \end{aligned}$$

where $r_i$ are in $R$, $r_i = r_i' + r_i''$, $r_i'$ are in $R^G$, and $r_i''$ are in $R_G$. The last equality follows since $S$ is a compatible $G$ and $R^G$-module: we apply (2.8) to get $\Sigma r_i' x_i$ in $S^G$ and $\Sigma r_i'' x_i$ in $S^G$. But

$$s = \Sigma r_i x_i + \Sigma r_i'' x_i$$

and $S = S^G \oplus S_G$, whence $\Sigma r_i'' x_i = 0$. Hence, $S^G$ is generated as an $R^G$-module by $\{x_i, \ldots, x_n\}$.

(c) Suppose that $R \cdot S^G$ is a finite and projective $R$-module. Then as in (b) $R \cdot S^G = \Sigma_{i=1}^n Rx_i$ where the $x_i$ are in $S^G$. Define

$$\theta\colon\ R^{(n)} \to R \cdot S^G \quad \text{by} \quad \theta(r_1, \ldots, r_n) = \Sigma_{i=1}^n r_i x_i .$$

Clearly, $\theta$ is a surjective $R$-morphism. Also $\theta$ is a $G$-morphism:

$$\begin{aligned} \theta(g(r_1, \ldots, r_n)) &= \theta(gr_1, \ldots, gr_n) \\ &= \Sigma g(r_i) x_i \\ &= \Sigma g(r_i g(x_i)) \\ &= g(\Sigma r_i x_i) \\ &= g(\theta(r_1, \ldots, r_n)) \end{aligned}$$

for all $g$ in $G$.

Now $R\cdot S^G$ a projective $R$-module implies that the following exact sequence of $R$-modules splits:

$$0 \to N \to R^{(n)} \xrightarrow{\theta} R\cdot S^G \to 0$$

where $N = \text{kernel}(\theta)$. Hence, $R^{(n)} \cong N\oplus R\cdot S^G$ as $R$-modules. Since $N$ is the kernel of a $G$-morphism, $N$ is not only an $R$-module but also a $G$-module. So we have

$$\begin{aligned}(R^G)^{(n)}\oplus(R_G)^{(n)} &\cong (R^G\oplus R_G)^{(n)} \\ &\cong R^{(n)} \\ &\cong N\oplus R\cdot S^G \\ &\cong N^G\oplus N_G\oplus S^G\oplus(R\cdot S^G)_G \\ &\cong (N^G\oplus S^G)\oplus(N_G\oplus(R\cdot S^G)_G)\end{aligned}$$

as $R^G$-modules since $N^G$, $S^G$, $N_G$, and $(R\cdot S^G)_G$ are $R^G$-modules by (2.8). By (2.9) $N_G\oplus(R\cdot S^G)_G$ is $G$-ergodic. Thus, since

$$((R^G)^{(n)}\oplus(R_G)^{(n)})^G = (R^G)^{(n)}$$

and

$$(N^G\oplus S^G\oplus N_G\oplus(R\cdot S^G)_G)^G = N^G\oplus S^G,$$

we have that

$$(R^G)^{(n)} \cong N^G\oplus S^G$$

as $R^G$-modules.

(d) Suppose that $S$ is a strongly separable $R$-algebra and that $S^G$ is a separable $R^G$-algebra. By (1.2) $R\cdot S^G$ is a strongly separable $R$-algebra. In particular, $R\cdot S^G$ is a finite and projective $R$-module. By (c) $S^G$ is a finite and projective $R^G$-module. Hence, $S^G$ is a strongly separable $R^G$-algebra.

Since $G$ is linearly reductive, applying (2.8), we have that $R^G \to R$ and $S^G \to S$ are split monomorphisms as $R^G$ and $S^G$-modules respectively. If $S$ is a strongly separable $R$-algebra, then $R \to S$ is a split $R$-monomorphism [DI, 4.2, P.56]. In the case that we have a linearly reductive finite group $\Gamma$ with $S^\Gamma = R$ and $(S^G)^\Gamma = R^G$, then $R^G = (S^G)^\Gamma \to S^G$ is a split $R^G$-monomorphism. We need the next result [F, J.6, P.157].

(2.11) Let $T$ be any commutative $R^G$-algebra. Then $G$ operates by $T$-algebra automorphisms on $R\otimes_{R^G}T$ and the action is rational. Moreover,

$$(R\otimes_{R^G}T)^G = T.$$

Let $T$ be an $R^G$-algebra. Then $S^G\otimes_{R^G}T$ is an $S^G$-algebra. By (2.11), replacing $R$ with $S$ and $T$ with $S^G\otimes_{R^G}T$, we find that $G$ acts rationally on

$$S\otimes_{S^G}(S^G\otimes_{R^G}T) = S\otimes_{R^G}T \quad\text{and}\quad (S\otimes_{R^G}T)^G = (S\otimes_{S^G}(S^G\otimes_{R^G}T))^G$$
$$= S^G\otimes_{R^G}T.$$

Hence, if we have a G-diagram:

$$\begin{tikzcd}[arrows=dash] & S \arrow[dl] \arrow[dr] & \\ S^G \arrow[dr] & & R \arrow[dl] \\ & R^G & \end{tikzcd}$$

we may "tensor" to get a new G-diagram:

$$\begin{tikzcd}[arrows=dash] & S\otimes_{R^G}T \arrow[dl] \arrow[dr] & \\ S^G\otimes_{R^G}T \arrow[dr] & & R\otimes_{R^G}T \arrow[dl] \\ & T=R^G\otimes_{R^G}T & \end{tikzcd}$$

For $S^G \hookrightarrow S$, $R \hookrightarrow S$, and $R^G \hookrightarrow R$ are all split $R^G$-monomorphisms; hence, $S^G\otimes T$ is contained in $S\otimes T$, $R\otimes T$ in $S\otimes T$, and $T$ in $R\otimes T$. But since

$$T = (R\otimes T)^G \subseteq (S\otimes T)^G = S^G\otimes T,$$

we have that $T$ is contained in $S^G\otimes T$. So, for instance, we can take $T = R^G/m$ where $m$ is in $\mathrm{Max}(R^G)$ and reduce to a G-diagram with $R^G$ a field.

We now examine a major theorem of this chapter. As we noted in (1.2), $R \cdot S^G$ plays an important role regarding the separability of $S^G$ as an $R^G$-algebra. In fact, in the Reductive Case the separability of $S^G$ as an $R^G$-algebra is completely determined by $R \cdot S^G$.

Theorem 2.12: Suppose that we have a G-diagram of $S$ over $R$ in the Reductive Case with $S$ a strongly separable R-algebra. Then $S^G$ is a strongly separable $R^G$-algebra if and only if $S$ is a projective $R \cdot S^G$-module.

Proof: If $S^G$ is a strongly separable $R^G$-algebra, then by (1.2) $S$ is a projective $R \cdot S^G$-module.

Conversely, assume that $S$ is a projective $R \cdot S^G$-module. Hence, since $S$ is a strongly separable R-algebra, $R \cdot S^G$ is a strongly separable R-algebra [DI, 2.4, P.94]. By (1.5)

$$\text{nilrad}(R \cdot S^G) = \text{nilrad}(R) R \cdot S^G = \text{nilrad}(R) S^G$$

since nilrad(R) is an R-module. Since nilpotents map to nilpotents via automorphisms, nilrad(R) is a rational G-module. Hence,

$$\begin{aligned} \text{nilrad}(R) &= (\text{nilradR}))^G \oplus (\text{nilrad}(R))_G \\ &= \text{nilrad}(R^G) \oplus (\text{nilrad}(R))_G, \end{aligned}$$

and

$$\begin{aligned} \mathrm{nilrad}(R\cdot S^G) &= \mathrm{nilrad}(R)S^G \\ &= \mathrm{nilrad}(R^G)S^G \oplus (\mathrm{nilrad}(R))_G S^G. \end{aligned}$$

Note that $\mathrm{nilrad}(R^G)S^G$ is contained in $S^G$ and since $S_G$ is an $S^G$-module, $(\mathrm{nilrad}(R))_G S^G$ is contained in $S_G$. Therefore,

$$\begin{aligned} \mathrm{nilrad}(S^G) &= \mathrm{nilrad}(R\cdot S^G) \cap S^G \\ &= \mathrm{nilrad}(R^G)S^G. \end{aligned}$$

Let $m$ be in $\mathrm{Max}(R^G)$ and reduce to the G-diagram:

$$\begin{tikzcd}[column sep=small] & R\cdot S^G\otimes R^G/m \arrow[dl, dash] \arrow[dr, dash] & \\ S^G\otimes R^G/m \arrow[dr, dash] & & R\otimes R^G/m \arrow[dl, dash] \\ & R^G/m & \end{tikzcd}$$

Note that $R\cdot S^G\otimes R^G/m$ is a strongly separable $R\otimes R^G/m$-algebra [DI, 1.11, P.46], and $R\cdot S^G\otimes R^G/m = (R\otimes R^G/m) \otimes (S^G\otimes R^G/m)$. By the above

$$\begin{aligned} \mathrm{nilrad}(S^G\otimes R^G/m) &= \mathrm{nilrad}(R^G/m)(R\cdot S^G\otimes R^G/m) \\ &= 0. \end{aligned}$$

Since $R\cdot S^G\otimes R^G/m$ is a finite $R$-module, by (2.10b) $S^G\otimes R^G/m$ is a finite $R^G/m$-module. By (2.5) $R$ a finitely generated $k$-algebra and $G$ linearly reductive implies that $R^G$ is a finitely generated k-algebra. Hence, by the Nullstellensatz $R^G/m = k$, an algebraically closed field. This means that we have $S^G \otimes R^G/m$ a reduced, finite dimensional $R^G/m$ vector space with $R^G/m$ algebraically closed. Thus $S^G \otimes R^G/m$ is a separable $R^G/m$-algebra [DI, 2.5, P.50]. Hence, with this happening for each $m$ in $\mathrm{Max}(R^G)$, $S^G$ is a separable $R^G$-algebra [DI, 71., P.72]. And by (2.10d) $S^G$ is a strongly separable $R^G$-algebra.

Remark 2.13: Suppose that we have a G-diagram of S over R as in the Reductive Case with S a strongly separable R-algebra. If $R \subseteq S^G$, then $S^G$ is a strongly separable $R = R^G$-algebra. Note that in this case S is a strongly separable $S^G$-algebra. Hence, by [VZ', 1.3] since R has only finitely many idempotents, G is finite. So if G is infinite, this setting cannot happen.

Proof: Since $R \subseteq S^G$, $R = R^G$. Note that $S^G$ is a finite R-module. For if $\{x_1,\ldots,x_n\}$ generates S as an R-module, then for s in $S^G$

$$
\begin{aligned}
s &= \Sigma r_i x_i \\
&= \Sigma r_i x_i' + r_i x_i'' \\
&= \Sigma r_i x_i'
\end{aligned}
$$

with $r_i$ in R, $x_i' + x_i'' = x_i$, $x_i'$ in $S^G$, and $x_i''$ in $S_G$. The last equality follows since $\Sigma r_i x_i'$ is in $S^G$ and $\Sigma r_i x_i''$ is in $S_G$ by (2.8). Hence, $S^G$ is generated as an R-module by $\{x_1',\ldots,x_n'\}$.

Since $R = R^G$, the G-diagram collapses to

$$\begin{array}{c} S \\ | \\ S^G \\ | \\ R = R^G. \end{array}$$

Let $m$ be in $\mathrm{Max}(R)$ and reduce to the following G-diagram:

$$\begin{array}{c} S \otimes R/m \\ | \\ S^G \otimes R/m \\ | \\ R/m = k. \end{array}$$

Now $S \otimes R/m$ is a separable extension of the field $R/m = k$. Hence, $S \otimes R/m$ is reduced, and so $S^G \otimes R/m$ is reduced and a finite extension of the algebraically closed field $R/m = k$. Thus $S^G \otimes R/m$ is a separable $R/m$-algebra. Since $S^G$ is a finite $R$-module, $S^G$ is a separable $R$-algebra, and by (2.10d) $S^G$ is a strongly separable $R$-algebra.

Theorem 2.14: Suppose that we have a G-diagram of $S$ over $R$ as in the Reductive Case and $S$ is a strongly separable $R$-algebra. If $G$ is finite and $R/mR = R \otimes_{R^G} R^G/m$ is reduced for all $m$ in $\mathrm{Max}(R^G)$, then $S^G$ is a strongly separable $R^G$-algebra.

Proof: Since $G$ is finite, $S$ is integral over $S^G$ and $R$ is integral over $R^G$. Hence, with $S$ and $R$ finitely generated $S^G$ and $R^G$-algebras respectively, $S$ is a finite $S^G$-module and $R$ is a finite $R^G$-module. Let $m$ be in $\mathrm{Max}(R^G)$ and reduce to the following diagram:

$$\begin{tikzcd} & S\otimes_{R^G} R^G/m \arrow[dl, dash] \arrow[dr, dash] & \\ S^G\otimes_{R^G} R^G/m \arrow[dr, dash] & & R\otimes_{R^G} R^G/m \arrow[dl, dash] \\ & R^G/m = k. & \end{tikzcd}$$

Since $R\otimes R^G/m$ is reduced and finite over the algebraically closed field $R^G/m = k$, $R\otimes R^G/m$ is a separable $R^G/m$-algebra. Hence, $R$ is a separable $R^G$-algebra and with $G$ finite, a strongly separable $R^G$-algebra [K]. This implies that $S$ is a strongly separable $R^G$-algebra. But $R^G \subseteq S^G \subseteq S$. So $S$ is a separable $S^G$-algebra. But again $G$ is finite; and so $S$ is a strongly separable $S^G$-algebra. Therefore, $S^G$ is a strongly separable $R^G$-algebra.

<u>Theorem 2.15</u>: Suppose that we have a G-diagram of $S$ over $R$ as in the Reductive Case with $S$ a strongly separable $R$-algebra and a finite group $\Gamma$ contained in the automorphisms of $S$ such that $S^\Gamma = R$ and $(S^G)^\Gamma = R^G$. If for each $m$ in $\mathrm{Max}(R^G)$, $R/mR = R\otimes_{R^G} R^G/m$ is reduced, then $S^G$ is a strongly separable $R^G$-algebra.

<u>Proof</u>: By (2.10a) $S^G$ is a finite $R^G$-module. Let $m$

be in $\mathrm{Max}(R^G)$ and reduce to the following G-diagram:

$$\begin{tikzcd}[column sep=small]
 & S\otimes_{R^G}R^G/m \arrow[dl, dash] \arrow[dr, dash] & \\
S^G\otimes_{R^G}R^G/m \arrow[dr, dash] & & R\otimes_{R^G}R^G/m \arrow[dl, dash] \\
 & R^G/m. &
\end{tikzcd}$$

Since $S\otimes R^G/m$ is a strongly separable $R\otimes R^G/m$-algebra, applying (1.5) we find that

$$\mathrm{nilrad}(S\otimes R^G/m) = \mathrm{nilrad}(R\otimes R^G/m)(S\otimes R^G/m) = 0.$$

Hence, $S^G\otimes R^G/m$ is reduced and finite over the algebraically closed field $R^G/m$. Thus $S^G\otimes R^G/m$ is a separable $R^G/m$-algebra. Since this is true for all $m$ in $\mathrm{Max}(R^G)$ and $S^G$ is a finite $R^G$-module, $S^G$ is a separable $R^G$-algebra [DI, 7.1, P.72], and by (2.10d) $S^G$ is also a finite and projective $R^G$-module.

Note that in (21.4) and (2.15) we could reduce to the case in which $S^G$ had no non-zero nilpotents. But we needed either $G$ finite or a $\Gamma$ to insure that $S^G$ was a finite $R^G$-module.

We now examine the Galois question regarding $S^G$ and $R^G$.

Theorem 2.16: Suppose that we have a G-diagram of S over R as in the Reductive Case and S is a Galois extension of R with group $\Gamma$ such that $(S^G)^\Gamma = R^G$. Then $S^G$ is a Galois extension of $R^G$ with group $\Gamma|S^G$ if and only if $R\cdot S^G$ is a Galois extension of R with group $\Gamma|R\cdot S^G$.

Proof: If $S^G$ is a Galois extension of $R^G$, by (1.2) $R\cdot S^G$ is a Galois extension of R.

Conversely, assume that $R\cdot S^G$ is a Galois extension of R with group $\Gamma|R\cdot S^G$. Hence,

$$\ell: \; R\cdot S^G \otimes_R R\cdot S^G \to C(\Gamma|R\cdot S^G,\, R\cdot S^G)$$

by

$$\ell(a\otimes b)(\gamma) = a\gamma(b)$$

is an isomorphism. Since $(S^G)^\Gamma = R^G$, by (1.1) we need only show that $\ell'$: $S^G \otimes_{R^G} S^G \to C(\Gamma|S^G,\, S^G)$ defined by $\ell'(a\otimes b)(\gamma) = a\gamma(b)$ is surjective. Note that we have the following commutative diagram:

$$\begin{tikzcd}
R\cdot S^G \otimes_R R\cdot S^G \arrow[r, "\ell"] & C(\Gamma|R\cdot S^G,\, R\cdot S^G) \\
S^G \otimes_{R^G} S^G \arrow[u, "\alpha"] \arrow[r, "\ell'"] & C(\Gamma|S^G,\, S^G) \arrow[u, hook, "j"']
\end{tikzcd}$$

where $\alpha(a\otimes_{R^G} b) = a\otimes_R b$ and j is the inclusion. Let f be in $C(\Gamma|S^G,\, S^G)$. Since $\ell$ is surjective,

$f = \ell(\Sigma r_i s_i \otimes t_i)$ where we may assume that the $r_i$ are in $R$ and the $s_i, t_i$ are in $S^G$; for

$$f = \ell(\Sigma x_i \otimes y_i), \quad \text{for } x_i \text{ and } y_i \text{ in } S,$$
$$= \ell(\Sigma r_i' s_i \otimes r_i'' t_i), \text{ for } r_i' \text{ and } r_i'' \text{ in } R,$$
$$= \ell(\Sigma r_i s_i \otimes t_i), \quad \text{for } r_i = r_i' r_i'' .$$

Hence, for eacn $\gamma$ in $\Gamma$,

$$f(\gamma) = \ell(\Sigma r_i s_i \otimes t_i)(\gamma)$$
$$= \Sigma r_i s_i \gamma(t_i)$$
$$= \Sigma r_i^* s_i \gamma(t_i) + r_i^{**} s_i \gamma(t_i)$$

where $r_i^* + r_i^{**} = r_i$, $r_i^*$ is in $R^G$, and $r_i^{**}$ is in $R_G$. But $s_i\gamma(t_i)$ is in $S^G$, and so by (2.8) $\Sigma r_i^{**} s_i \gamma(t_i)$ is in $S_G$. But $f(\gamma)$ is in $S^G$. Hence, $\Sigma r_i^{**} s_i \gamma(t_i) = 0$, and $f(\gamma) = \Sigma r_i^* s_i \gamma(t_i)$. This means that

$$f = \ell'(\Sigma r_i^* s_i \otimes t_i),$$

i.e,. $\ell'$ is surjective.

<u>Corollary 2.17</u>: Let the setting be as in (2.16). If $\Gamma | R\cdot S^G = \Gamma$, then $S^G$ is a Galois extension of $R^G$ with group $\Gamma$ if and only if $S$ is invariantly generated over $R$.

<u>Proof</u>: If $S$ is invariantly generated over $R$, then the corollary follows from (2.16).

Conversely, if $S^G$ is a Galois extension of $R^G$, we apply (1.11) to get that $S = R\cdot S^G$.

Corollary 2.18: Let the setting be as in (2.16). Also, assume that $S^G$ has no idempotents but 0,1. Then $S^G$ is a Galois extension of $R^G$ with group $\Gamma|S^G$ if and only if $S$ is a projective $R\cdot S^G$-module.

Proof: If $S^G$ is a Galois extension of $R^G$, then $S^G$ is a strongly separable $R^G$-algebra. By (1.2) $S$ is a projective $R\cdot S^G$-module.

Conversely, if $S$ is a projective $R\cdot S^G$-module, then $S^G$ is a strongly separable $R^G$-algebra by (2.12). But with $(S^G)^\Gamma = R^G$ and $S^G$ having no non-trivial idempotents, $S^G$ is a Galois extension of $R^G$ with group $\Gamma|S^G$.

Note that in the setting of (2.18) that $R\cdot S^G$ is a Galois extension of $R$ if and only if $S$ is a projective $R\cdot S^G$-module by (2.16). Also, in (1.22) the conditions of the Reductive Case were satisfied; hence, $S^G$ a Galois extension of $R^G$ does not imply that $S$ is a Galois extension of $R$. We now end the chapter with an example in which $S$ is a Galois extension of $R$, yet $S^G$ is a finite $R^G$-module but not a separable $R^G$-algebra. But first a lemma:

Lemma 2.19: Let

$$R = k[x_1, x_2, 1/x_1] = k[x_1, x_2, x_3]/\langle x_1x_3 - 1\rangle$$

and

$$S = k[x_1, x_2, 1/x_1^{1/m}] = R[y]/\langle y^m - x_1\rangle ,$$

where $m$ is even and relatively prime to the characteristic of $k$ which may not be $2$. Then $S$ is a Galois extension of $R$.

<u>Proof</u>: Since $k$ is algebraically closed, $k$ contains all its $m^{th}$ roots of unity. Let $\xi$ be a primitive $m^{th}$ root of unity. Then

$$\Gamma = \{\sigma_0, \ldots, \sigma_{m-1} \mid \sigma_i(x_1^{1/m}) = \xi^i x_1^{1/m}\}$$

is a finite group of automorphisms of $S$. Since $\Gamma$ fixes $x_1$, $x_2$, and $1/x_1$ but does not fix $(x_1^{1/m})^i$ for $i = 0, \ldots, m-1$, $S^\Gamma = R$. Let $y = x_1^{1/m}$. Then

$$\Sigma_{i=0}^{m-1}(1/m \cdot y^i)\sigma_j(y^{-i}) = \delta_{\sigma_j, 1}$$

since $1 - (\xi^j)^m = (\xi^j - 1)(1 + \xi^j + \ldots + \xi^{j(m-1}) = 0$ with $\xi^j - 1 \neq 0$, which implies, if $j \neq 0$, that

$$\begin{aligned} 0 &= 1 + \xi^j + \ldots + \xi^{j(m-1} \\ &= \Sigma_{i=0}^{m-1}(1/m \cdot y^i)(\sigma_j(y^{-i})). \end{aligned}$$

And if $j = 0$, then

$$\begin{aligned} \Sigma_{i=0}^{m-1}(1/m \cdot y^i)(\sigma_0(y^{-i})) &= 1/m\Sigma_{i=0}^{m-1}\, y^i y^{-i} \\ &= 1/m\Sigma_{i=0}^{m-1}\, 1 \\ &= 1/m \cdot m \\ &= 1. \end{aligned}$$

Note by Maschke's Theorem [CR, P.41] since the order of $\Gamma$ is $m$ which is relatively prime to the characteristic of $k$, that $\Gamma$ is linearly reductive.

Now for the example:

(2.20) Let $R$, $S$, and $\Gamma$ be as in (2.19); and let $G = GL_1(k) = k^*$, the units of $k$. $G$ is linearly reductive [F, 5.24, P.172]. Define the action of $G$ on $S$ by

$$t(x_1) = t^{l_1}x_1,$$

$$t(x_2) = t^{l_2}x_2,$$

for $t$ in $G$ where $l_1, l_2 > 0$ and $ml_2$ divides $l_1$. Note that

$$t(1/x_1) = t^{-l_1}(1/x_1)$$

and

$$t(x_1^{1/m}) = t^{l_1/m}x_1^{1/m} .$$

Since the action of $G$ is linear, $S$ is a rational $G$-module.

An arbitrary element of $R$ looks like

$$\sum\sum\sum_{i,j,k\geq 0} a_{ijk}\, x_1^i x_2^j (1/x_1)^k = \sum\sum\sum_{i,j,k\geq 0} a_{ijk}\, x_1^{i-k} x_2^j$$

(*) $$= \sum_{j\geq 0,i}\sum b_{ij}\, x_1^i x_2^j$$

Thus if $t$ is in $G$, then

$$t\Big(\sum_{j\geq 0,i}\sum b_{ij}\, x_1^i x_2^j\Big) = \sum_{j\geq 0,i}\sum b_{ij}\, t^{il_1} x_1^i t^{jl_2} x_2^j$$

$$= \sum_{j\geq 0,i}\sum b_{ij}\, t^{il_1+jl_2} x_1^i x_2^j \ .$$

Hence, (*) is in $R^G$ if and only if $il_1+jl_2 = 0$. So

$$R^G = \Big\{\sum_{j\geq 0,i}\sum b_{ij}\, x_1^i x_2^j \,\Big|\, il_1 + jl_2 = 0\Big\}$$

$$= \Big\{\sum_{i\leq 0} c_i\, x_1^i x_2^{-il_1/l_2}\Big\}$$

$$= \Big\{\sum_{i\leq 0} c_i\, (x_2^{l_1/l_2}/x_1)^{-i}\Big\}$$

$$\Big\{\sum_{i\geq 0} c_{-i}\, (x_2^{l_1/l_2}/x_1)^{i}\Big\} \ .$$

An arbitrary element of $S$ looks like

$$\sum\sum\sum\sum_{i,j,k,s\geq 0} a_{ijks}\, x_1^i x_2^j (1/x_1)^k (x_1^{1/m})^s = \sum\sum\sum\sum_{i,j,k,s\geq 0} a_{ijks}\, x_1^{i-k} x_2^j (x_1^{1/m})^s$$

$$= \sum\sum\sum\sum_{i,j,k,s\geq 0} a_{ijks}\, (x_1^{1/m})^{m(i-k)+s} x_2^j$$

$$(**) \qquad = \sum_{j\geq 0,i}\sum b_{ij}\, (x_1^{1/m})^i x_2^j \ .$$

Hence, (**) is in $S^G$ if and only if $(il_1/m)+jl_2 = 0$. So

$$S^G = \{\sum_{j\geq 0,i} \sum b_{ij} x_1^{i/m} x_2^j \mid (il_1/m)+jl_2 = 0\}$$

$$= \{\sum_{i\leq 0} c_i (x_1^{1/m})^i x_2^{-il_1/ml_2}\}$$

$$= \{\sum_{i\geq 0} c_{-i} (x_2^{l_1/ml_2}/x_1^{1/m})^i\} \quad .$$

Let $z = x_2^{l_1/l_2}/x_1$ and $w = x_2^{l_1/ml_2}/x_1^{1/m}$. Then $z = w^m$ or $w = z^{1/m}$. Thus we may think of $R^G = k[z]$ and $S^G = k[z,z^{1/m}] = R^G[w]/< w^m-z >$. But $m$ is a unit and $z$ is not a unit in $S^G$, hence, $S^G$ is not a separable $R^G$-algebra [W, 1.8] and [J, 2.2].

From (2.12) we know that the example must fail because $R\cdot S^G$ is "bad" in this case:

$$R\cdot S^G = (k[x_1,x_2,1/x_1])(k[x_2^{l_1/l_2}/x_1, x_2^{l_1/ml_2}/x_1^{1/m}]$$

$$= k[x_1,x_2,1/x_1,x_2^{l_1/ml_2}/x_1^{1/m}]$$

$$= R[w]/< w^m - x_2^{l_1/l_2}/x_1 >.$$

And $m$ is a unit in $R\cdot S^G$ but $x_2^{l_1/l_2}/x_1$ is not. Hence, $R\cdot S^G$ is not a separable $R$-algebra, and $S$ is not a projective $R\cdot S^G$-module.

BIBLIOGRAPHY


[B] Bourbaki, N., Commutative Algebra, Addison-Wesley, Reading, Masschusetts, 1972.

[CR] Curtis, C.W. and Reiner, I., Representation Theory of Finite Groups and Associative Algebras, Interscience, New York, 1962.

[CHR] Chase, S.U., Harrison, D.K. and Rosenberg, A., Galois Theory and Cohomology of Commutative Rings, Mem. Amer. Math. Soc. 52 (1965).

[DI] DeMeyer, F. and Ingraham, E., Separable Algebras over Commutative Rings, Math Lecture Notes #181, Springer-Verlag, New York, 1971.

[F] Fogarty, J., Invariant Theory, W.A. Benjamin Inc., New York, 1969.

[I] Ingraham, E., Inertial Subalgebras of Algebras over Commutative Rings, Trans. Amer. Math. Soc. 124 (1966), 77-93.

[J] Janusz, G., Separable Algebras over Commutative Rings, Trans. Amer. Math. Soc. 122 (1966), 461-479.

[K] Kreimer, H.F., Automorphisms of Commutative Rings, Trans. Amer. Math. Soc. 203 (1975), 77-85.

[L] Lang, S., Algebra, Addison-Wesley, Reading, Massachusetts, 1971.

[M] Magid, A., The Separable Galois Theory of Commutative Rings, Marcel Dekker, Inc., New York, 1974.

[N] Nagahara, T., A Note on Galois Theory of Commutative Rings, Proc. Amer. Math. Soc. 18 (1967), 334-340.

[VZ'] Villamayor, O.E. and Zelinsky, D., Galois Theory for Rings with Finitely Many Idempotents, Nagoya Math.J. 27 (1966), 721-731.

[VZ"] _______, _____, Galois Theory with Infinitely Many Idempotents, Nagoya Math J. 35 (1969), 83-98.

[W] Wang, S., Separable Algebras over Commutative Rings, to appear.