PACIFIC JOURNAL OF MATHEMATICS
Vol. 36, No. 2, 1971

DIVISOR CLASSES IN PSEUDO GALOIS EXTENSIONS

WILLIAM C. WATERHOUSE

Let R be a Krull domain with fraction field K. Let L be a finite extension of K, and let S be the integral closure of R in L; then S is also a Krull domain. Let $\mathscr{P}(R, S)$ be the group of divisor classes in R becoming principal in S. Suppose there is a group scheme (or Hopf algebra) acting on S with fixed ring R. Then there is a cohomology group which contains $\mathscr{P}(R, S)$ and equals it if the action is Galois at each minimal prime. This generalizes and unifies some results of Samuel.

1. Definition of the cohomology group. Let R, K, L and S be as above. Let H be a cocommutative Hopf algebra over R, with δ, ε, and ρ its comultiplication, counit, and coinverse. One calls S an *H-module algebra* [9, p. 207] if it has an H-module structure such that $h \cdot 1 = \varepsilon(h)$ and $h \cdot (ss') = \sum (h_i \cdot s)(h'_i \cdot s')$ where $\delta(h) = \sum h_i \otimes h'_i$. We say that R is the fixed ring in S if

$$R = \{s \in S \mid h \cdot s = \varepsilon(h)s \quad \text{for all} \quad h \in H\} .$$

In this case L is naturally an H-module algebra with fixed ring K.

Suppose now S is an H-module algebra with fixed ring R, and consider the set

$$\{b \in L^* \mid b^{-1}(h \cdot b) \in S \quad \text{for all} \quad h \in H\} .$$

This is a group under multiplication: if b and c are in it, we have

$$(bc)^{-1}h \cdot (bc) = \sum (b^{-1}h_i \cdot b)(c^{-1}h'_i \cdot c)$$

and

$$(h \cdot b^{-1})b = \sum h_i \cdot [b^{-1}(\rho h'_i) \cdot b] .$$

It contains S^* and K^* as subgroups. We write $H^0(H, L^*/S^*)$ for its quotient by S^*, and $\mathscr{Q}(H, S)$ for the quotient by S^*K^*. Note that $h \mapsto b^{-1}h \cdot b$ defines a function $H \to S$; it is easy to check that b and c give the same function if and only if bc^{-1} is in the fixed ring K, and hence we can also view $\mathscr{Q}$ as these functions modulo the functions coming from units $b \in S^*$.

PROPOSITION 1. *Assume S is an H-module algebra with fixed ring R. Then there is a canonical injection*

$$\mathscr{P}(R, S) \to \mathscr{Q}(H, S) .$$

Proof. Let D be a divisorial ideal of R with div (DS) principal, say $= bS$. Let P be a minimal prime of R, and choose $r \in K$ with $\mathrm{ord}_P\, r = \mathrm{ord}_P\, D$; then $bS_P = rS_P$. For any $h \in H$ we have

$$h \cdot b \in h \cdot rS_P = rh \cdot S_P \subseteq rS_P = bS_P \ ,$$

and hence $b^{-1}h \cdot b \in \bigcap_P S_P = S$. The element b is well determined up to multiplication by an element of S^*, and thus we have a map (obviously a homomorphism) from such ideals D to $H^0(H, L^*/S^*)$. Since div $(DS) = S$ implies $D = R$, the map is injective. Divide now by K^* in both places.

One can define [9] a sequence of cohomology groups $H^i(H, S^*)$. In that theory $H^1(H, S^*)$ consists of certain equivalence classes of functions $H \to S$; it maps naturally to $H^1(H, L^*)$, and the kernel comprises functions of the form $h \mapsto b^{-1}h \cdot b$. Under our hypotheses also $H^0(H, S^*) = R^*$ and $H^0(H, L^*) = K^*$. Thus our group $H^0(H, L^*/S^*)$ fits into an exact sequence, and $\mathscr{C}(H, S)$ is its image in $H^1(H, S^*)$.

Suppose that G is a group, $H = R[G]$. To make S an H-module algebra is simply to let G act as R-algebra automorphisms of S. The definition of fixed ring is then the usual one, and $H^0(H, L^*/S^*)$ is the subset of L^*/S^* fixed by G. In addition [9, p. 211], the cohomology $H^1(H, S^*)$ is naturally isomorphic to $H^1(G, S^*)$.

Suppose on the other hand that H is the polynomial ring $R[X]$, with $\delta(X) = X \otimes 1 + 1 \otimes X$, $\varepsilon(X) = 0$, and $\rho(X) = -X$. Then an H-module algebra structure is given by an R-linear derivation $D: S \to S$ (where $Ds = X \cdot s$). The fixed ring is $\{s \mid Ds = 0\}$. The values $b^{-1}h \cdot b$ are determined by $b^{-1}Db$, and all lie in S if this one does; hence $\mathscr{C}(H, S)$ can be identified with the logarithmic derivatives Db/b lying in S, modulo the logarithmic derivatives of elements of S^*. Thus it is the group introduced by Samuel in [7, p. 86], and our formalism unifies the two separate theories he presents. We could similarly take a finite set of derivations, let H be an enveloping algebra for them, and get the group used in [10] and [11]. (The paper [11] contains a different connection between Samuel's group and cohomology, but it appears to be *ad hoc* rather than natural.)

Suppose that H is *finite*, i.e., a finitely generated projective R-module; this is the most important case. Let $A = \mathrm{Hom}\,(H, R)$ be the linear dual, a commutative Hopf algebra. Making S an H-module algebra is then the same thing as giving an algebra homomorphism $\sigma: S \to A \otimes_R S$ suitably compatible with the comultiplication and counit of A (cf. [5, p. 33]); in geometric language, this is an action of the finite group scheme Spec A on Spec S over Spec R. In these terms

$$\mathscr{C}(H, S) = \{\sigma(b)b^{-1} \mid b \in L^*, \sigma(b)b^{-1} \in (A \otimes S)^*\}/S^* \ ;$$

the group $H^1(H, S^*)$ is the quotient by S^* of the equalizer of two homomorphisms from $(A \otimes S)^*$ to $(A \otimes A \otimes S)^*$, and so on. One could phrase all the results equally well in terms of A, and I have used H only because it is closer to the language used in the literature.

2. Conditions for isomorphism. Assume S is an H-module algebra with H finite. We say that S with this structure is *Galois* if the following equivalent conditions hold [5, p. 66]:

(I) S is a finitely generated projective R-module, and the map $H \otimes_R S \rightarrow \mathrm{End}_R S$ given by $h \otimes s_0 \mapsto [s \mapsto s_0 h \cdot s]$ is an R-module isomorphism.

(II) S is a faithfully flat R-module, and

$$(\sigma, 1 \otimes id_S): S \otimes_R S \longrightarrow A \otimes_R S$$

is an R-algebra isomorphism. In geometric language, this says [6, p. 27] that Spec S is a principal homogeneous space for Spec A. It implies that R is the fixed ring.

PROPOSITION 2. *Suppose H is finite. If L is Galois as an $H \otimes_R K$-module algebra, then*

$$\mathscr{Q}(H, S) = H^1(H, S^*) .$$

Proof. This will follow if we show that $H^1(H, L^*) = 0$. But it is easy to see from the definition (cf. end of § 1) that this group equals $H^1(H \otimes K, L^*)$, which since the structure is Galois equals [9, p. 219] the Amitsur cohomology $H^1(L/K, \mathbf{G}_m)$; this is 0 by the generalized Hilbert Theorem 90 [1, p. 96 or 6, p. 15].

THEOREM 1. *Assume S is an H-module algebra with H finite. The following are equivalent:*

(i) *For all minimal primes P of R, the H_P-structure on S_P is Galois.*

(ii) *R is the fixed ring, and for all minimal primes P of R the H_P/PH_P-structure on S_P/PS_P is Galois.*

(iii) *R is the fixed ring, and for all minimal primes P of R the map*

$$S_P/PS_P \otimes S_P/PS_P \rightarrow A_P/PA_P \otimes S_P/PS_P$$

is an isomorphism.

(iv) *The map $S \otimes S \rightarrow A \otimes S$ is a pseudo-isomorphism [in the sense that its R-module kernel and cokernel vanish when localized to any minimal prime]. These conditions imply*

(v) *R is the fixed ring, and the map $H \otimes S \rightarrow \mathrm{End}_R S$ is a* *pseudo-isomorphism; they are equivalent to it if we assume either R Noetherian or S a finitely generated R-module.*

Proof. If (i) holds then R is the fixed ring because $R = \bigcap R_P$. Obviously (i) is equivalent to (iv), which implies (iii); and (iii) is equivalent to (ii) since A_P/PA_P is the R_P/PR_P-dual of H_P/PH_P. If we now assume (ii) we have $\dim H_P/PH_P = \dim S_P/PS_P$. We know [3, p. 147] that the latter is $\leqq |L: K|$, with equality only if S_P is a free R_P-module. But we also know that K is the fixed ring in L, and it follows [9, p. 219] that $\dim H_P/PH_P = \dim_K H \otimes K \geqq |L: K|$. Hence we conclude that S_P is free. But then the map $S_P \otimes S_P \rightarrow A_P \otimes S_P$, which is an isomorphism modulo P, is an actual isomorphism by Nakayama's lemma.

As for (v), we have the diagram

$$\begin{array}{ccc} (H \otimes S)_P & \longrightarrow & (\operatorname{End} S)_P \\ \Vert & & \downarrow \\ H_P \otimes S_P & \longrightarrow & \operatorname{End}(S_P) \end{array} ,$$

where we know that the arrow on the right is injective for any S and surjective if S is finitely generated [4, p. 49]. If we assume (i) we have an isomorphism on the bottom, and hence we must have an isomorphism on the top; if S is finitely generated we can reverse the implication.

We claim now that $(\operatorname{End}_R S) \otimes K = \operatorname{End}_K L$ if and only if S is an R-lattice in L. Indeed, if S is an R-lattice, then $\operatorname{End}_R S$ is an R-lattice in $\operatorname{End}_K L$ by [4, p. 45]. For the converse let $1 = s_1, s_2, \cdots, s_n$ be a basis of L, and consider the maps $\varphi_i: \sum \alpha_j s_j \mapsto (\alpha_i)1$. If $\operatorname{End}_R S$ is sufficiently large there is a $0 \neq r \in R$ such that the $r\varphi_i$ map S into S, and then $S \subseteqq (1/r)(Rs_1 + \cdots + Rs_n)$.

Now assume (v) with R Noetherian. The fact that K is the fixed ring implies again that $\operatorname{rank}(H) \geqq |L: K|$, so by dimension count $(\operatorname{End} S) \otimes K$ is all of $\operatorname{End}_K L$. Then S is an R-lattice, hence finitely generated, and the earlier argument applies.

If the conditions of the theorem hold, we say that S with its H-structure is *pseudo-Galois*. One result of the proof deserves to be noted:

Porism. If R is Noetherian and S is pseudo-Galois, then S is finitely generated over R.

THEOREM 2. *Assume that S is a pseudo-Galois H-module algebra. Then*

$$\mathscr{P}(R, S) \cong \mathscr{Q}(R, S) \cong H^1(H, S^*) .$$

Proof. We know (by further localization) that L is Galois for $H \otimes K$, so the second isomorphism is just Proposition 2. Take now a $b \in L^*$ with $h \cdot b \in bS$ for all $h \in H$; we must prove that bS comes from a divisor of R. This is a local statement, so we may assume that R is a discrete valuation ring and S is Galois. It follows then that bS is mapped to itself by all elements of $\operatorname{End}_R S$. Choose a basis $s_1, \cdots, s_n$ of S and elements $r_1, \cdots, r_n$ in K such that $r_1 s_1, \cdots, r_n s_n$ is a basis of bS; permuting the s_i, we see that $bS = r_1 S$.

COROLLARY 1. *Suppose L is a Galois field extension of K with group G, and assume that all the minimal primes of R are unramified in S. Then S is pseudo-Galois for $R[G]$, and hence*

$$\mathscr{P}(R, S) \cong H^1(G, S^*) .$$

Proof. The fact that S_P is Galois for $R_P[G]$ when there is no ramification is a well-known bit of folklore; much more general results are proved, e.g., in [2].

COROLLARY 2. *Suppose L over K is purely inseparable of degree p, and D is a K-derivation with $DS \subseteq S$. Let $H = R[X]$ as above, and let H_0 be the image of H in* End S. *Assume DS is not contained in any minimal prime of S. Then S is pseudo-Galois for H_0, and hence*

$$\mathscr{P}(R, S) \cong \mathscr{Q}(H_0, S) \cong \mathscr{Q}(H, S) .$$

Proof. The hypotheses imply readily that $D^p = \lambda D$ for some $\lambda \in R$ [8, p. 63], and we have $H_0 \cong R[X]/(X^p - \lambda X)$. Functions $h \mapsto b^{-1}h \cdot b$ are equal on H if and only if they are equal on H_0, so the second isomorphism is trivial. To prove that S is pseudo-Galois we may localize and assume that R is a discrete valuation ring with maximal ideal P; by inseparability there is a unique maximal ideal Q of S lying over it. By hypothesis S/PS has a nontrivial derivation $\bar{D}$ over R/P; in particular the two cannot be equal, and so S/PS either is a p-dimensional field extension or has the form $(R/P)[Y]/Y^p$. In either case the hypothesis $DS \nsubseteq Q$ shows that $\bar{D}y$ is invertible for a generator y of S/PS. If D_1 is the derivation with $D_1 y = 1$, we have $D_1 = (1/\bar{D}y)\bar{D}$ in the image of $H_0/PH_0 \otimes S/PS$. But it is well known (and trivial) that D_1 and S/PS generate End S/PS. Thus the map from $H_0/PH_0 \otimes S/PS$ is a surjection, and dimension count shows it is an isomorphism.

The isomorphism $\mathscr{P} \cong \mathscr{Q}$ could be proved for these two cases by using the idea in Theorem 2, showing from the given hypotheses that an element b with $h \cdot b \in bS$ comes locally from R. This is essentially what is done in [7]. But our argument brings out the general result underlying Samuel's two theorems. It also yields the extension to several derivations in [10, Th. 2.9]. In addition, the example in the next section shows that we can treat problems (with $L^p \not\subseteq K$) which cannot be handled by derivations.

3. The surface $Z^q = XY$. Let k be a field of positive characteristic p, and let L be the fraction field of $S = k[x, y]$. Let q be a power of p, and let K be the fraction field of $R = k[x^q, y^q, xy]$. As in [8, p. 65], it is easy to see that $R = S \cap K$ and so is a Krull domain; it is the affine coordinate ring of $Z^q = XY$ with $x^q = X$ and $y^q = Y$. Let G be a cyclic group of order q, with generator g. Set $A = R[G]$ and map $S \to A \otimes_R S$ by $x \mapsto g \otimes x$ and $y \mapsto g^{-1} \otimes y$. Then the dual $H = R^G$ has a basis of idempotents $e_0, e_1, \cdots, e_{q-1}$ with $e_\lambda \cdot x^i y^j$ equal to $x^i y^j$ if $\lambda \equiv i - j \pmod q$ and equal to 0 otherwise. As an R-module, $S = \bigoplus e_i S$; the fixed ring is $e_0 S = R$.

The map $S \otimes S = \bigoplus e_i S \otimes S \to A \otimes S$ takes $s_i \otimes t$ to $g^i \otimes s_i t$ for $s_i \in e_i S$. Thus to show that S is pseudo-Galois we must show that the multiplication maps $e_i S \otimes S \to S$ are isomorphisms at each minimal prime P of R. Since L is purely inseparable over K, we know that S_P is a local ring; the condition then is that $e_i S$ contain a unit of S_P, i.e., not lie in the maximal ideal. But obviously $e_i S$, which contains both x^i and y^{q-i}, does not lie in any minimal ideal of $S = k[x, y]$. Hence S is pseudo-Galois for H.

Take now an element b with all $e_i b \in bS$; multiplying by an element of K^*, we may assume b is a polynomial. Then $e_i b$ consists of some of its terms, and for all these to be multiples of b requires that $b = e_i b$ for some i. All such elements are K-multiples of x^i, and these give us a cyclic group of order q. Since S has unique factorization, all divisors of R become principal, and we have proved

PROPOSITION 4. *Let k be a field of characteristic p, and q a power of p. Then the divisor class group of $k[x^q, y^q, xy]$ is cyclic of order q.*

We can carry out the same proof assuming only that k is a unique factorization domain, just as was done in [8, p. 65]. (The result could be proved there, of course, only for $q = p$.)

4. Galois extensions and the kernel of Pic. Among the divisorial ideals of R are the invertible ideals, and the group $\operatorname{Pic} R$ of invertible ideals modulo principal ideals is a subgroup of the divisor class group. Thus the kernel of the map $\operatorname{Pic} R \to \operatorname{Pic} S$ is a subgroup of $\mathscr{P}(R, S)$. In general it may well be smaller. In the example of § 3, for instance, $\mathscr{P}(R, S)$ is generated by the inverse image of xS, which [4, p. 89] is just $xS \cap R$; this is not an invertible ideal. Suppose however that S is flat over R. Then a divisorial ideal D is mapped simply to DS [4, p. 20]; since S is integral, it is faithfully flat over R, and so DS principal implies D invertible. Hence we have proved the following generalization of [10, Corollary 2.8]:

PROPOSITION 5. *Assume that S is a pseudo-Galois H-module algebra and is flat over R. Then*

$$\mathscr{C}(H, S) \cong \operatorname{Ker}(\operatorname{Pic} R \to \operatorname{Pic} S) .$$

These hypotheses are true if S is Galois for H. In fact, they nearly imply S Galois, as the following theorem shows.

THEOREM 3. *Assume S is a pseudo-Galois H-module algebra. The following are equivalent:*

(1) *S is Galois for H.*

(2) *S is a projective R-module.*

Proof. By definition (1) implies (2), so assume (2). In the proof of Theorem 1 we saw that S is an R-lattice; then $S \otimes S$ and $A \otimes S$ are projective R-lattices, and the map between them is an isomorphism at every minimal prime P.

To complete the proof we just recall that if M is a projective R-lattice in a K-space V, then M is finitely generated and $M = \bigcap M_P$. Since this result seems to have been omitted from [4], we sketch the proof. Writing M as a direct summand of a free module gives us linear functions $f_i: M \to R$ and elements $m_i \in M$ such that (*) $m = \sum f_i(m)m_i$ for all $m \in M$. There is a natural extension of f_i to a linear function $V \to K$, and (*) then holds for all $m \in V$. Let $v_1, \cdots, v_n$ be a basis of V, with dual basis $v_1^*, \cdots, v_n^*$, and write $f_i = \sum a_{ir} v_r^*$. Applying (*) to the v_r shows that $a_{ir} = 0$ for all but finitely many i; thus M is finitely generated. If $m \in \cap M_P$ then $f_i(m) \in \cap R_P = R$, so $m \in M$.

COROLLARY. *Assume R Noetherian, S pseudo-Galois and flat. Then S is Galois.*

Proof. We have S flat by hypothesis and finitely generated by the Porism to Theorem 1; hence S is projective.

REFERENCES

1. S. A. Amitsur. *Simple algebras and cohomology groups of arbitrary fields*, Trans. Amer. Math. Soc. **90** (1959), 73-112.

2. M. Auslander and O. Goldman, *The Brauer group of a commutative ring*, Trans. Amer. Math. Soc. **97** (1960), 367–409.
3. N. Bourbaki, *Algèbre Commutative*, Ch. 5, 6, Hermann, Paris, 1964.
4. ———, *Algèbre Commutative*, Ch. 7, Hermann, Paris, 1965.
5. S. U. Chase and M. E. Sweedler, *Hopf Algebras and Galois Theory*, ETH Springer Lecture Notes 97, Springer, New York, 1969.
6. A. Grothendieck, *Technique de descente et théorèmes d'existence en géométrie algébrique*, I. Sem. Bourbaki 190, 1959–1960, Benjamin, New York.
7. P. Samuel, *Classes de diviseurs et dérivées logarithmiques*, Topology **3** (1964), Suppl. 1, 81–96.
8. ———, *Lectures on Unique Factorization Domains*, Tata Institute Lectures 30, Bombay, 1964.
9. M. E. Sweedler, *Cohomology of algebras over Hopf algebras*, Trans. Amer. Math. Soc. **133** (1968), 205–239.
10. S. Yuan, *On logarithmic derivatives*, Bull. Soc. Math. France **96** (1968), 41–52.
11. N. Zinn-Justin, *Dérivations dans les corps et anneaux de charactéristique p*, Bull. Soc. Math. France Mémoire 10, 1967.

Received December 16, 1969.

CORNELL UNIVERSITY