Osaka University Knowledge Archive

Title	Galois theory and ideals in commutative rings
Author(s)	Kreimer, H. F.
Citation	Osaka Journal of Mathematics. 1975, 12(2), p. 441-448
Version Type	VoR
URL	https://doi.org/10.18910/5372
rights	
Note	

Osaka University Knowledge Archive : OUKA

https://ir.library.osaka-u.ac.jp/

Osaka University

Kreimer, H.F.
Osaka J. Math.
12 (1975), 441-448

GALOIS THEORY AND IDEALS IN COMMUTATIVE RINGS*

H.F. KREIMER

(Received May 7, 1974)

Introduction. Let A be a commutative ring with 1. For any ideal i of A, let $r(i)$ denote the radical of i, which is the set of all elements of A some power of which lies in i or, equivalently, the intersection of all prime ideals of A which contain i. If p is a prime ideal of A and X is a unital A-module, let X_p denote the module of fractions of X with respect to the complement of p in A. If q is a primary ideal of A; then $p=r(q)$ is a prime ideal of A and the ideal-length of q, denoted by $\lambda(q)$, is the length of a composition series for the A-module $A_p/q\,A_p$.

In the sequel, let B be a given commutative ring with 1, let G be a given finite group of automorphisms of B, and let A be the subring of G-invariant elements of B. For any prime ideal p in A, G is represented as a group of automorphisms of B_p by the formula $\sigma\left(\frac{b}{s}\right)=\frac{\sigma(b)}{s}$ for $\sigma\in$ G, $b\in B$, and $s\in A-p$ and A_p is the subring of G-invariant elements of B_p by [4, Chap. V, §1, Prop.

Abstract. Let B be a commutative ring with 1, Let G be a finite group of automorphisms of B, and let A be the subring of G-invariant elements of B. For an A-subalgebra A' of B, which has the property that A'_p is a separable A_p-algebra for every prime ideal p in A, the following assertions are proved. If q is a primary ideal of A; then $q\,A'$ has a unique irredundant representation as a finite intersection of primary ideals of A', each primary component of $q\,A'$ lies over q and has ideal-length equal to the ideal-length of q, and the associated prime ideals of $q\,A'$ are the prime ideals of A' which lie over the radical of q. If, in addition, A' is G-stable, then the contraction map is an isomorphism of the lattice of G-stable ideals of A' onto the lattice of ideals of A. Also it is demonstrated that there exists a maximal A-subalgebra A' of B which has the property that A'_p is a separable A_p-algebra for every prime ideal p in A, and this subalgebra is unique and G-stable.

AMS 1970 *subject classification.* Primary 13BO5, 13B10; Secondary 13A15, 13B15.
Key words and phrases. Automorphism, commutative ring, prime ideal, primary ideal, separable algebra.
* The author gratefully acknowledges support in his research from the National Science Foundation under grant #33027x.

23]. Letting A′ be an A-subalgebra of B, A'_p is an A_p-subalgebra of B_p and the following property will be considered.
(P) Ap is a separable A_p-algebra for every prime ideal p in A.
If A' satisfies property (P); then A'_p is a finitely generated, projective A_p-module for every prime ideal p in A, according to the main theorem of [8]. In particular, Ap is a flat A_p-module for every prime ideal p *in* A; and therefore A' is a flat A-module by [4, Chap. II, §3, Corollary to Prop. 15]. But let A' be any A-subalgebra of B which is a flat A-module. Since B is integral over A [4, Chap. V, §1, Prop. 22], A' must also be integral over A. Consequently, every prime ideal of A is the contraction of a prime ideal of A' [4, Chap. V, §2, Thm. 1], and A' is a faithfully flat A-mdule by [4, Chap. I, §3, Prop. 9]. Then for any ideal i of A, the inclusion map of i into A induces an isomorphism of $i\otimes_A A'$ onto $i\ A'$ since A' is a flat A-module, and $A\cap(iA')=i$ by [4, Chap. I, §3, Prop. 9]. Finally, if A' is an A-subalgebra of B which satisfies property (P); then A'_p/pA'_p is a separable $A_p/p\ A_p$-algebra by [3, Prop. 1.4], and so A' is an unramified A-algebra as defined in [1].

1. Ideal theory. Notice that for any ideal i of A, $B\ i$ is a G-stable ideal of B.

Theorem 1. *Assume that B satisfies property (P), i.e. B_p is a separable A_p-algebra for every prime ideal p in A. The mapping $I \rightsquigarrow A\cap /$ is an isomorphism of the lattice of G-stable ideals of B onto the lattice of ideals of A, and the inverse of this isomorphism is the mapping $i \rightsquigarrow i\ B$.*

Proof. It is evident that the mapping $I \rightsquigarrow A\cap I$ is a homomorphism of the lattice of G-stable ideals of B into the lattice of ideals of A; and, to complete the proof, it is only necessary to show that the mapping $i \rightsquigarrow i\ B$ from the lattice of ideals of A into the lattice of G-stable ideals of B is the inverse of this homomorphism. It was noted in the introduction that $A\cap i\ B=i$ for any ideal i of A, and it remains to show that $(A\cap I)\,B=I$ for every G-stable ideal I of B. Letting / be a G-stable ideal of B, however, $(A\cap I)\ B\subseteq I$; and $(A\cap I)B=I$ if and only if $[(A\cap I)\ B]_p=I_p$ for every prime ideal p in A [4, Chap. II, §3, Thm. 1]. Moreover, for any given prime ideal p of A, it is readily verified that I_p is a G-stable ideal of B_p, it follows from [4, Chap. II, §2, Prop. 18] that $[(A\cap I)\,B]_p=(A\cap I)_p B_p$, and $(A\cap I)_p=A_p\cap I_p$ by [4, Chap. II, §2, Remark following Thm. 1]. Consequently the proof may be restricted to the case in which B is a separable A-algebra. Accordingly, assume B is a separable A-algebra and let $\Omega=\mathrm{Hom}_A(B,B)$. Since Ω is generated as a left B-module by G [8, Prop. 3], / is a submodule of the left Ω-module B; and it is readily verified that the correspondence $f \rightsquigarrow f(1)$ is an A-module isomorphism of $\mathrm{Hom}_\Omega(B, /)$ onto $A\cap I$. Also B is a finitely generated, projective A-module by the main theorem of [8], and it follows from [2, Prop. A.3] that the trace ideal of B in A is all of A. Therefore the homomorphism of $(A\cap I)\otimes_A B$ into I, which maps $a\otimes b$ onto ab for $a\in A\cap I$ and $b\in B$, is an isomorphism by [2, Prop. A.6]; and so $(A\cap I)B=I$.

If A' is an A-subalgebra of B which is G-stable, then G may be represented as a group of automorphisms of A' for which A is the subring of invariant elements by restricting the elements of G to mappings on A'. Therefore theorem 1 may be applied to any G-stable, A-subalgebra of B which satisfies property (P).

Lemma. *Let i be an ideal of a commutative ring A such that $r(i)$ is the intersection of finitely many prime ideals of A.*

(i) *If p is a minimal element in the set of all prime ideals of A which contain i, then the set $q=\{x\in A\mid i:xA\not\subseteq p\}$ is a primary ideal of A and $r(q)=p$.*

(ii) *If $r(i)$ is the intersection of finitely many maximal ideals of A then i has a unique irredundant representation as a finite intersection of primay ideals of A, there are only finitely many maximal ideals of A which contain i, and they are the associated prime ideals of i.*

Proof. Let p be a prime ideal of A which contains i, and let $q=\{x\in A\mid i:xA\not\subseteq p\}$. Note that i_p is an ideal of A_p, while q is the contraction of i_p and it is the kernel of the canonical homomorphism of A into $(A/i)_{(p/i)}$ by [4, Chap. II, §2, Prop. 10 and Prop. 11]. If a and b are elements of A such that $ab\in q$, then there exists $c\in A$ such that $abc\in i$ but $c\notin p$. If $a\notin q$; then $i: aA\subseteq p$, in particular $bc\in p$, and so $b\in p$. Since $i\subseteq p$, $r(i)\subseteq p$; and, letting $p_1,\cdots,p_n$ be distinct prime ideals of A such that $r(i)=\bigcap_{k=1}^{n} p_k$, there must exist an integer k, $1\leq k\leq n$, such that $p_k\subseteq p$. Thus, if p is a minimal element in the set of all prime ideals of A which contain i; then $p=p_k$ for some integer k, $1\leq k\leq n$, say $p=p_1$, and $p_k\not\subseteq p$ for $k\neq 1$. Therefore $\bigcap_{k=2}^{n} p_k\not\subseteq p$, and there exists $c\in \prod_{k=2}^{n} p_k$ such that $c\notin p$. Now if $b\in p$, then $bc\in r(i)$ and there exists a positive integer m such that $b^m c^m\in i$. But since $c\notin p$, $c^m\notin p$ and therefore $b^m\in q$. Thus q is a primary ideal of A and $r(q)=p$ by [10, Chap. III, Thm. 13].

Now suppose that $p_1,\cdots,p_n$ are maximal ideals of A. In this case, if p is any prime ideal of A which contains i, then $p=p_k$ for some integer k, $1<k<n$. Therefore $p_1,\ \ ,p_n$ are the only prime ideals of A which contain i, and each of them is a minimal element in the set of all prime ideals of A which contain i. Setting $q_k=\{x\in A\mid i:xA\not\subseteq p_k\}$ for $1\leq i\leq n$, $i=\bigcap_{k=1}^{n} q_k$ since the canonical homomorphism of $A\backslash i$ into the direct product $\prod_{k=1}^{n}(A/i)_{(p_k/i)}$ is injective by [4,

Chap. II, §3, Cor. 2 to Thm. 1]. Thus a finite, irredundant primary representation for $\imath$, in which the primary components are isolated, is obtained; and this representation is unique by [10, Chap. IV, Thm. 8].

Theorem 2. *If A' is an unramified A-subalgebra of B and a flat A-module, and q is a primary ideal of A then :*

(i) *$q\ A'$ has a unique irredundant representation as a finite intersection of primary ideals of A'*

(ii) *The associated prime ideals of $q\ A'$ are the prime ideals of A' which lie over $r(q)$*

(iii) *The primary components of $q\ A'$ lie over q;*

(iv) *For any primary component q' of $q\circ A'$, $\lambda(q')=\lambda(q)$.*

Proof. Let A' be an unramified A-subalgebra of B which is a flat A-module, let q be a primary ideal of A, and let $p=r(q)$. Then $q\ A_p$ is a primary ideal of A_p, $p\ A_p$ is its radical, and q and p are contracted ideals by [10, Chap. IV, Thm. 16]. In particular, q is the kernel of the canonical homomorphism of A into $A_p/q\,A_p$. Since A' is a flat A-module, $q\otimes_A A'$ is naturally isomorphic to the kernel of the canonical homomorphism of A' into $A'p\backslash q\ A'_p$; and therefore $q\ A'$ is the contraction of the ideal $q\ A'_p$. Also, for any prime (resp. primary) ideal q' of A', $A\cap q'$ is a prime (resp. primary) ideal of A, $(A\cap q' A_p=A_p\cap(q'A_p)$ by [4, Chap. II, §2, Remark following Thm. 1], and $\lambda(q')=\lambda(q'A_p)$ while $\lambda(q)=\lambda(qA_p)$ by [10, Chap. IV, Cor. to Thm. 26]. It now follows from [10, Chap. IV, Thm. 15, Thm. 16, and their corollaries] that if the theorem is verified for the ideals $q\ A_p$ and $q\ A'_p$, then it is true for the ideals q and $q\ A'$. Thus it is sufficient to prove the theorem under the additional assumptions that A is a local ring, $p=r(q)$ is the unique maximal ideal of A, and A'/pA' is a separable algebra over the field A/p. Then $A'/p\ A'$ is a finite dimensional algebra over $A\backslash p$ by [9, Prop. 1.1], it is a semi-simple algebra by [5, Chap. IX, Prop. 7.3 and Prop. 7.7], and it follows readily that $p\ A'$ is an intersection of finitely many maximal ideals of A'. Consequently $p\ A'$ must be the radical of $q\ A'$; and by the preceding lemma, $q\ A'$ has a unique irredundant representation as a finite intersection of primary ideals of A' and the associated prime ideals of $q\ A'$ are the maximal ideals of A' which contain $q\ A'$.

Any prime ideal of A' which lies over p contains $q\ A'$, and therefore it must coincide with one of the maximal ideals of A' which is an associated prime of $q\ A'$ [10, Chap. IV, Thm. 7]. Now let q' be a primary component of $q\ A'$ and let $p'=r(q')$. Then $A\cap p'$ must coincide with the maximal ideal $p=r(q)$. According to the proof of the preceding lemma or [10, Chap. IV, Thm. 8]

$q'=\{x\in A' \mid qA' : xA' \nsubseteq p'\}$, while $q=\{x\in A \mid q: xA \nsubseteq p\}$ since q is a primary ideal. Given $x\in A$, $(q: xA)\ A'=(q\ A': xA')$ by [4, Chap. I, §2, remark following Cor. 2 to Prop. 12], since A' is a flat A-module. If $x\notin q$; then $q: xA\subseteq p$, $q\ A':\ xA'\subseteq p\ A'\subseteq p'$, *and* $x\notin q'$. Thus $A\cap q'\subseteq q$, but clearly $q=A\cap qA'\subseteq A\cap q'$, and so $A\cap q'=q$. Since A is a local ring with unique maximal ideal p, $A_p=A$ and $\lambda(q)$ is the length of a composition series for the A-module A/q. Let i and j be ideals of A such that $q\subseteq j\subseteq i\subseteq p$ and i/j is isomorphic as an A-module to A/p. Since $A'_{p'}$ is a flat A-module by [4, Chap. II, §3, Prop. 14]; $q\ A'_{p'}\subseteq j\ A'_{p'}\subseteq i\cdot A'_{p'}\subseteq p\cdot A'_{p'}$ and $i\circ A'_{p'}/j\cdot A'_{p'}\simeq(i/j)\otimes_A A'_{p'}\simeq(A/p)\otimes_A A'_{p'}\simeq A'_{p'}/p\ A'_{p'}$ as A'-modules. But $p\ A'_{p'}=(p\circ A')\cdot A'_{p'}$ coincides with the maximal ideal $p'\cdot A'_{p'}$ of $A'_{p'}$ by [10, Chap. IV, Thm. 17], and it then follows readily that $\lambda(q)=\lambda(q')$.

As indicated in the introduction, any A-subalgebra of B which satisfies property (P) will satisfy the hypotheses of theorem 2.

2. Examples and an existence theorem. The purpose of this section is to investigate further the property (P). The following example shows that the ring B may satisfy property (P) but fail to be a separable A-algebra.

EXAMPLE 1. Consider a ring of infinite sequences of complex numbers with the usual component-wise addition and multiplication of sequences, and let B be the subring of those infinite sequences for which all but finitely many terms of the sequence are real and equal. An automorphism σ of B is determined by assigning to each element b of B the infinite sequence whose terms are complex conjugates of the terms of b, and σ^2 is the identity map on B. Letting G be the group consisting of σ and the identity automorphism of B, the subring A of G-invariant elements of B consists of all infinite sequences of real numbers for which all but finitely many terms of the sequence are equal. For any prime ideal p in A, it is readily verified that either there exists a positive integer k such that p consists of all elements of A with zero k-th term, in which case B_p is isomorphic to the field of complex numbers and A_p is isomorphic to the subfield of real numbers, or p consists of all elements of A with only finitely many non-zero terms, in which case B_p and A_p are equal and isomorphic to the field of real numbers. Therefore B satisfies property (P). But it is also easily seen that B is not a finitely generated A-module. As a consequence of the main theorem of [8], B is not a separable A-algebra.

The next example demonstrates that B may be an unramified A-algebra and a flat A-module, but fail to satisfy property (P). Thus property (P) is a sufficient but not necessary condition for the conclusions of theorem 2 to be obtained.

EXAMPLE 2. Let Φ be a field of characteristic not equal to two, and let $\{x_i \mid i=1,2, \cdots\}$ be a countably infinite set of elements which are algebraically independent over Φ. Letting B_i be the localization of $\Phi[x_i]$ with respect to its maxmimal ideal (x_i), the Φ-algebra homomorphism of $\Phi[x_i]$ into $\Phi[x_{i+1}]$ which maps x_i onto x_{i+1}^3 has a unique extension to a homomorphism of B_i into B_{i+1}. Using these homomorphisms, the direct limit B of the rings B_i may be formed; and letting ω_i be the canonical homomorphism of B_i into B and $y_i=\omega_i(x_i)$, $y_i=y_{i+1}^3$ for $i=1, 2, \cdots$. For each positive integer i, the Φ-algebra automorphism of $\Phi[x_i]$ which maps x_i onto $-x_i$ has a unique extension to an automorphism of B_i; and these automorphisms determine a Φ-algebra automorphism σ of B such that $\sigma(y_i)=-y_i$ and σ^2 is the identity map. Let G be the group consisting of σ and the identity automorphism, and let A be the subring of G-invariant elements of B. For a given positive integer i, consider the subring $A[y_i]$ of B. Since $y_i^2 \in A$, $A[y_i]$ is generated as an A-module by its elements 1 and y_i. If tfo+^ij'*—0 for a_0, $a_1 \in A$, then $a_0-a_1y_i=\sigma(a_0+a_1y_i)=0$. Adding the two equations, $2a_0=0$; and hence $a_0=0$ and $a_1=0$. Thus 1 and y_i freely generate the A-module $A[y_i]$; and, in particular, $A[y_i]$ is a flat A-module. Also, since $y_i=y_{i+1}^3$, $A[y_i] \subseteq A[y_{i+1}]$. Consequently, B is the union of its subrings $A[y_i]$, $i=1, 2, \cdots$; and B is a flat A-module by [4, Chap. I, §2, Prop. 2].

Now let P be a prime ideal of B and let $p=A \cap P$. If P is the zero ideal of B; then $A_p/pA_p \simeq A_p$ is the field of fractions of A, and from [4, Chap. V, §1, Prop. 23] it follows that $B_p/pB_p \simeq B_p$ is the field of fractions of B and A_p is the subfield of G-invariant elements of B_p. In that case, B_p/pB_p is a separable field extension of A_p/pA_p. Henceforth, assume that P is a proper prime ideal of B. Then there must exist a positive integer k such that $\omega_i^{-1}(P)$ is a proper prime ideal of B_k. The only proper prime ideals of $\Phi[x_k]$ are its maximal ideals, however, and so, by [4, Chap. II, §2, Prop. 11] there can be only one proper prime ideal of B_k and it is generated by x_k. Therefore $y_k \in P$, and from the equations $y_i=y_{i+1}^3$ it follows that $y_i \in P$ for every positive integer i. But it is readily verified that the ideal of B generated by the y_i, $i=1, 2, \cdots$, is a maximal ideal with a residue class ring which is naturally isomorphic to Φ and so P must be this ideal. Then p is a maximal ideal of A by [4, Chap. V, §2, Prop. 1], and there exist natural isomorphisms of A_p/pA_p onto A/p and $B_p/pB_p \simeq (A_p/pA_p) \otimes_A B$ onto $B/p \cdot B \simeq (A/p) \otimes_A B$ by [4, Chap. II, §3, Prop. 2]. Since $y_{i+1}^2 \in p$ and $y_i=y_{i+1}^3 \in B \cdot p$ for every positive integer i, $Bp=P$ and $B/Bp=B/P=\Phi=A/p$. Again in this instance, B_p/pB_p is a separable field extension of A_p/pA_p; and consequently B is an unramified A-algebra. Also A and B are local rings with maximal ideals p and P respectively, and hence the A-algebra B satisfies property (P) only if B is a separable A-algebra. Since B has no non-trivial idempoetnt elements; were B a separable A-algebra, B would be a Galois extension of A with Galois group G by [6, Thm. 1.3]. But then the canonical representation of G as a group of automorphisms of $E\backslash P$ would be faithful by [7, Thm. 1.4], and yet σ induces the identity automorphism on B/P. Therefore B is not a separable A-algebra.

The property (P), however, admits the following theorem.

Theorem 3. *There exists an A-subalgebra of B which satisfies property* (P), *is stable under G, and contains every other A-subalgebra of B satisfying property* (P).

Proof. Let p be any given prime ideal of A; and notice that if A' is an A-subalgebra of B for which A'_p is a separable A_p-algebra, for instance if A satisfies property (P), then A'_p is a free A_p-module whose rank does not exceed the order of the group G by the main theorem of [8]. Partially order the A-subalgebras of B which satisfy property (P) by inclusion, let F be a chain of such subalgebras of B, and let $\bar{A}=\bigcup_{A'\in F} A'$. For the given prime ideal p of A, choose an element A' of P so that the rank of the A_p-module A'_p is as large as possible. If B' is an element of F such that $A'\subseteq B'$; then $A'_p\subseteq B'_p$, and, as a consequence of [8, Lemma 1], B'_p/A'_p is also a free A_p-module and $\operatorname{rank}(A'_p)+\operatorname{rank}(B'_p/A'_p)=\operatorname{rank}(B'_p)$. But because of the choice of A'; $\operatorname{rank}(A'_p)=\operatorname{rank}(B'_p)$, $\operatorname{rank}(B'_p/A'_p)=0$, and $A'_p=B'_p$. Consequently $\bar{A}_p=A'_p$, and A_p is a separable A_p-algebra. Thus it is seen that the A-algebra A satisfies property (P), and certainly it is an upper bound for F. By Zorn's Lemma, there exists a maximal A-subalgebras C of B satisfying property (P). Now let A' be any A-subalgebra of B which satisfies property (P). Since $(A'\ C)_p$ is a homomorphic image of the tensor product of the A_p-algebras A'_p and C_p, it is a separable A_p-algebra by [3, Prop. 1.4 and Prop. 1.5]. Thus $A'\ C$ satisfies property (P), and so $A'\cdot C=C$ or $A'\subset C$. Letting $\sigma\in G$, σ induces an A_p-algebra isomorphism of C_p onto $\sigma(C_p)$, and thus $\sigma(C_p)$ is a separable A_p-algebra. Therefore $\sigma(C)$ satisfies property (P), and so $\sigma(C)\subseteq C$.

FLORIDA STATE UNIVERSITY

References

[1] M. Auslander and D. A. Buchsbaum: *On ramification theory in Noetherian rings,* Amer. J. Math. 81 (1959), 749-765.

[2] M. Auslander and O. Goldman: *Maximal orders,* Trans. Amer. Math. Soc. 97 (1960), 1-24.

[3]————: *The Brauer group of a commutative ring,* Trans. Amer. Math. Soc. 97 (1960), 367–409.

[4] N. Bourbaki: Algebra Commutative, Hermann, Paris, 1961.

[5] H. Cartan and S. Eilenberg: Homological Algebra, Princeton University Press, Princeton, N. J. 1956.

[6] S.U. Chase, D.K. Harrison, and A. Rosenberg: *Galois theory and cohomology of commutative rings,* Mem. Amer. Math. Soc. No. 52 (1965), 15-33.

[7] H.F. Kreimer: *Galois theory for noncommutative rings and normal bases,* Trans. Amer. Math. Soc. 127 (1967), 42–49.

[8]————: *Automorphisms of commutative rings*, Trans. Amer. Math. Soc. 203 (1975), 77-85.

[9] O.E. Villamayor and D. Zelinsky: *Galois theory for rings with finitely many idempotents,* Nagoya Math. J. 27 (1966), 721-731.

[10] O. Zariski and P. Samuel: Commutative Algebra, Vol. 1, D. Van Nostrand Co. Inc. Princeton, N.J. 1958.