Math, J. Okayama Univ. 26 (1984), 43—48

SOME p-GALOIS EXTENSIONS OF COMMUTATIVE RINGS

MITSURU SANEMASA

Throughout this paper, all rings and algebras will be assumed to be commutative with identity element. Moreover, R will mean an algebra over the prime field $GF(p)$ of characteristic $p>0$, and all ring extensions of R will be assumed with identity element 1 coinciding with the identity element of R. Let G be a finite p-group and $\Phi(G)$ the Frattini subgroup of G. For $r \in R$, we define $\mathscr{P}(r) = r^p - r$ and $\mathscr{P}(R) = \{\mathscr{P}(r);\ r \in R\}$. Then $R/\mathscr{P}(R)$ will always be considered as a vector space over $GF(p)$.

In [3], K. Kishimoto proved the following theorem which is a generalization of a main result in W. Witt [9] to connected rings, i.e., rings with no idempotents other than 1 and 0, and moreover, this is related to the results of D. J. Saltman [7], T. Nagahara and A. Nakajima [4].

Theorem (KISHIMOTO). *For a connected ring R, the following conditions are equivalent.*

(i) *There exists a G-Galois extension S of R such that S is a connected ring.*

(ii) *There exists a $G/\Phi(G)$-Galois extension M of R such that M is a connected ring.*

(iii) *$(R: \mathscr{P}(R))$, the index of the additive subgrovp $\mathscr{P}(R)$ of the additive group R, is not smaller than $(G : \Phi(G))$.*

The purpose of this paper is to generalize the above Kishimoto's result to some types of non-connected rings.

As in [8], $B(R)$ will mean the Boolean ring consisting of all idempotents in R, and Spec $B(R)$ will mean the Boolean spectrum of R which is a Stone space consisting of all prime ideals of $B(R)$. The family of the subsets $U_e = \{y \in \text{Spec } B(R); e \in y\}$ $(e \in B(R))$ forms a base of the open subsets of Spec $B(R)$. Now, let x be an element of Spec $B(R)$. we shall use R_x to denote the ring of residue classes of R modulo the ideal Rx, where Rx is the ideal of R generated by the elements of x. Then R_x is a connected ring ([8, (2.13]). Let M be an R-module. Then M_x will denote the tensor probuct $M \otimes_R R_x$, and for any element $a \in M$, a_x will denote the image of a under the canonical homomorphism $M \to M_x$.

First, we prepare some lemmas which have been used in the proofs of [5].

Lemma 1. *Let S be a ring extension of R. Then S_x is connected for every $x \in$ Spec $B(R)$ if and only if $B(R) = B(S)$.*

Proof. Suppose that S_x is connected for every $x \in$ Spec $B(R)$. Let $e \in B(S)$. Then, for any $x \in$ Spec $B(R)$, we have $e_x \in \{0_x, 1_x\}$, and so, $R_x + (eR)_x = R_x$. Therefore, it follows from [8, (2.11)] that $R + eR = R$, which shows $e \in R$. Thus, we obtain $B(S) = B(R)$. The converse is obvious.

Lemma 2. *R is a regular ring (in the sense of Von Neumann) if and only if R_x is a field for each $x \in$ Spec $B(R)$.*

Proof. See [6].

Lemma 3. *Let S be a separable extension of R. If $B(S) = B(R)$ and R is a regular ring, then S is a regular ring.*

Proof. Let $x \in$ Spec $B(R)$. Then S_x is a separable extension of R_x. Since R is a regular ring, R_x is a field by Lemma 2, and since $B(S) = B(R)$, S_x is connected by Lemma 1. Thus S_x is a field for every $x \in$ Spec $B(S)$, and so, S is a regular ring.

By virtue of the above lemmas, we can generalize Kishimoto's result [3, Theorem 2.2].

Theorem 1. *Let S be a G-Galois extension of R and M the fixring of $\Phi(G)$ in S. Then, $B(M) = B(R)$ if and only if $B(S) = B(R)$. Moreover, if $B(M) = B(R)$ and R is a regular ring, then S is a regular ring.*

Proof. Let $x \in$ Spec $B(R)$. Then S_x is a G-Galois extension of R_x and M_x is the fixring of $\Phi(G)$ in S_x. If $B(M) = B(R)$ then M_x is connected and by [3, Theorem 2.2], S_x is connected, whence, it follows from Lemma 1 that $B(S) = B(R)$. Combining this with Lemma 3, we obtain the second assertion.

This theorem has been proved by Nagahara and Nakajima in the case that G is abelian ([5]).

Now, Let $R[X_1, \cdots, X_k]$ be the ring of polynomials in variables $X_1, \cdots, X_k$ with coefficients in R. For $r_1, \cdots, r_k \in R$, define $R[\mathscr{P}^{-1}(r_i); 1 \leqq i \leqq k] = R[X_1, \cdots, X_k]/I$, where I is the ideal generated by $\{\mathscr{P}(X_i) - r_i;\ 1 \leqq i \leqq k\}$.

Let A be an elementary abelian group, i.e., $A = (\sigma_1) \times \cdots \times (\sigma_k)$ with (σ_i) of order p. Then, M is an A-Galois extension of R if and only if M is isomorphic to $R[\mathscr{P}^{-1}(r_i); 1 \leqq i \leqq k]$ for some $r_1, \cdots, r_k \in R$ ([7, Theorem 1.5]). When this is the case, M is connected if and only if R is connected and $r_1 + \mathscr{P}(R), \cdots, r_k + \mathscr{P}(R)$ are linearly independent in $R/\mathscr{P}(R)$ over $GF(p)$ ([7, Theorem 1.7]).

As a partial generalization of Kishimoto's result [3, Theorem 2.3(I)], we have the following

Theorem 2. *Let A be an abelian group which is isomorphic to $G/\Phi(G)$. Then, the following conditions are equivalent.*

(i) *There exists a G-Galois extension S of R with $B(M) = B(R)$.*

(ii) *There exists an A-Galois extension M of R with $B(M) = B(R)$.*

Moreover, if one of these conditions is satisfied, then $(R_x: \mathscr{P}(R_x)) \geqq (G: \Phi(G))$ for every $x \in$ Spec $B(R)$.

Proof. It is trivial that (i) implies (ii). Let G be of order p^m, and assume (ii). First, by induction methods, we shall prove that (ii) implies (i). If $p^m = p$ then the assertion is clear. Thus, we assume that $p^m > p$, and the implication (ii) $\Rightarrow$ (i) is true for any p-group whose order is small than p^m. Then $\Phi(G) \neq 1$. Hence, there exists a central subgroup C of order p which is contained in $\Phi(G)$. We put $p = G/C$. Then $\Phi(P) = \Phi(G)/C$ and $G/\Phi(G) \cong P/\Phi(P)$. By assumption, there exists a $P/\Phi(P)$-Galois extension M of R with $B(M) = B(R)$. Since p is of order p^{m-1}, it follows from induction hypothesis that there exists a P-Galois extension T of R with $B(T) = B(R)$. We can imbed T/R into a G-Galois extension S/R such that $S^C = T$ where S^C is the fixring of C in S ([7, Lemma 1.8(a)]). Since $T \supset S^{\Phi(G)}$, we obtain $B(S^{\Phi(G)}) = B(R)$ and so $B(S) = B(R)$ by Theorem 1. Next, we shall prove the last assertion. Since A is an elementary abelian group, we have $M \cong R[\mathscr{P}^{-1}(r_i); 1 \leqq i \leqq k]$ for some $r_1, \cdots, r_k \in R$, where p^k is the order of A. Now, let x be an arbitrary element of spec $B(R)$. Then, since $B(M) = B(R)$, $M_x \cong R_x[\mathscr{P}^{-1}(r_{ix}); 1 \leqq i \leqq k]$ is connected. Hence $r_{1x} + \mathscr{P}(R_x), \cdots, r_{kx} + \mathscr{P}(R_x)$ are linearly independent in $R_x/\mathscr{P}(R_x)$ over $GF(p)$. Thus, we obtain $(R_x: \mathscr{P}(R_x)) \geqq p^k = (G: \Phi(G))$.

Now, we introduce the notions of a uniform polynomial and a weakly uniform ring which were defined in F. DeMeyer [1].

First, let R be a connected ring. Then R has a locally strongly separable, connected R-algebra Γ (unique up to isomorphism) so that any finite subset of Γ is contained in a (projective) extension $R[\alpha_1, \cdots, \alpha_n]$ of R in Γ with α_i the root of a separable polynomial over $R[\alpha_1, \cdots, \alpha_{i-1}]$ and so that any separable polynomial over Γ factors into linear factors in Γ. Such algebra Γ will be called a polynomial closure of R. If $p(X)$ is a separable polynomial in $R(X)$ and $p(X) = (X-\alpha_1)\cdots(X-\alpha_n)$ in $\Gamma[X]$ then $R[\alpha_1, \cdots, \alpha_n]$ is a Galois extension of R whose Galois group consists of all R-automorphisms, and this group will be denoted by $G(p(X))$.

Next, let R be an arbitrary ring, and $y \in \text{Spec } B(R)$. Then, the natural homomorphism from R onto R_y induces a homomorphism from $R[X]$ to $R_y[X]$. For $p(X) \in R[X]$, we denote the corresponding polynomial in $R_y[X]$ by $p_y[X]$. A separable polynomial $p(X) \in R[X]$ is called to be uniform if for each $x \in \text{Spec } B(R)$, there exists a neighbourhood U of x in Spec $B(R)$ such that for all $y \in U$, $G(p_y(X)) \cong G(p_x(X))$. For any uniform separable polynomial in $R]X]$, there exists a finite projective separable extension N of R such that $p(X) = (X_1-\alpha_1)\cdots(X-\alpha_n)$ in $N[X]$, $N = R[\alpha_1, \cdots, \alpha_n]$ and $B(N) = B(R)$. Such N will be called a splitting ring for $p(X)$.

If χ is a topological space and Λ is a ring we let $C(\chi, \Lambda)$ be the ring of continuous functions from χ to Λ where Λ is with the topology such that point sets are open. A ring R will be called to be weakly uniform if there is a finite collection of totally disconnected compact Hausdorff spaces $\{\chi_1, \cdots, \chi_n\}$ and connected rings $\{\Lambda_1, \cdots, \Lambda_n\}$ such that R is ring isomorphic to the direct product of rings $C(\chi_i, \Lambda_i)$, $i = 1, \cdots, n$.

Now, we shall prove the following theorem which contains Kishimoto's result [3, Theorem 2.3(I)].

Theorem 3. *Let R be a weakly uniform ring, and A an abelian group which is isomorphic to $G/\Phi(G)$. Then, the following conditions are equivalent.*

(i) *There exists a G-Galois extension S of R which is weakly uniform and satisfies $B(S) = B(R)$.*

(ii) *There exists an A-Galois extension M of R which is weakly uniform and satisfies $B(M) = B(R)$.*

(iii) $(R_x\colon \mathscr{P}(R_x)) \geqq (G\colon \Phi(G))$ *for every* $x \in \text{Spec } B(R)$.

Proof. It is obvious by Theorem 2 that (i) implies (iii). We show that (iii) implies (ii). Let $(G\colon \Phi(G)) = p^k$, and $x \in \text{Spec } B(R)$. Then, there exist elements $r_1, \cdots r_k \in R$ such that $r_{1x} + \mathscr{P}(R_x), \cdots, r_{kx} + \mathscr{P}(R_x)$ are linearly independent in $R_x/\mathscr{P}(R_x)$ over $GF(p)$. Hence we obtain

(1) $$a_1 r_{1x} + \cdots + a_k r_{kx} \notin \mathscr{P}(R_x)$$

for every $(a_1, \cdots, a_k) \in GF(p)^{k*} = GF(p)^k \setminus \{(0, \cdots, 0)\}$, the complement of $\{(0, \cdots, 0)\}$ in the k-times product of $GF(p)$. Now, for an element $(a_1, \cdots, a_n) \in GF(p)^{k*}$, we set $r = a_1 r_1 + \cdots + a_k r_k$. Since $X^p - X - r$ is a separable polynomial over the weakly uniform ring R ([4, Lemma 1.1]), $X^p - X - r$ is a uniform polynomial ([1, Corollary 2.4]). Hence $\{y \in \text{Spec } B(R); r_y \notin \mathscr{P}(R_y)\}$ is an open set in Spec $B(R)$ containing x ([5, Proposition 2.1]). Note that $GF(p)^{k*}$ is a finite set. Then, by (1), there exists an open neighbourhood V of x such that

(2) $$a_1 r_{1y} + \cdots + a_k r_{ky} \notin \mathscr{P}(R_y) \text{ for all } y \in V$$

where $(a_1, \cdots, a_k)$ runs over all the elements in $GF(p)^{k*}$. Thus, for each $x \in \text{Spec } B(R)$, we obtain apair $(V, (r_1, \cdots, r_k))$ of an open neighbourhood V of x in Spec $B(R)$ and an element $(r_1, \cdots, r_k)$ of R^k which satisfies (2). Therefore, by partition property of Spec $B(R)$ (see [6, p.12]), we can find a finite subset $\{e_1, \cdots, e_n\}$ of $B(R)$ and a subset $\{(r_{1j}, \cdots, r_{kj}); j = 1, \cdots, n\}$ of R^k such that

$$U_{e_i} \cap U_{e_j} = \phi \text{ if } i \neq j,$$
$$\bigcup_{j=1}^{n} U_{e_j} = \text{Spec } B(R), \text{ and}$$
$$a_1(r_{1j})_y + \cdots + a_k(r_{kj})_y \notin \mathscr{P}(R_y) \text{ for all } y \in U_{e_j}$$

where $(a_1, \cdots, a_k)$ runs over all the elements in $GF(p)^{k*}$, and $U_{e_j} = \{y \in \text{Spec } B(R); e_j \in y\}$ $(j = 1, \cdots, n)$. Now, let be y an arbitrary element of Spec$\cdot B(R)$. Then, there exists $h \in \{1, \cdots, k\}$ such that $y \in U_{e_h}$ and $y \notin U_{e_j}$ if $j \neq h$. Clearly $(1 - e_h)_y = 1_y$ and $(1 - e_j)_y = 0_y$ for all $j \neq h$. We set here $s_i = \sum_{j=1}^{n} (1 - e_j) r_{ij}$. It follows then that

$$\left(\sum_{i=1}^{k} a_i s_i\right)_y = \sum_{i=1}^{k} a_i \sum_{j=1}^{n} (1 - e_j)_y (r_{ij})_y = \sum_{i=1}^{k} a_i (r_{ih})_y \notin \mathscr{P}(R_y)$$

for all $(a_1, \cdots, a_k) \in GF(p)^{k*}$. In other words, $s_{1y} + \mathscr{P}(R_y), \cdots, s_{ky} + \mathscr{P}(R_y)$ are linearly independent in $R_y / \mathscr{P}(R_y)$ over $GF(p)$. Thus $M = R[\mathscr{P}^{-1}(s_i); 1 \leqq i \leqq k]$ is an A-Galois extension of R such that $M_y = R_y[\mathscr{P}^{-1}(s_{iy}); 1 \leqq i \leqq k]$ is connected. Since y is arbitrary in Spec $B(R)$, this implies $B(M) = B(R)$ by Lemma 1. We put $R_0 = R$ and $R_i = R_{i-1}[\mathscr{P}^{-1}(r_i)]$ $(1 \leqq i \leqq k)$. Since R_1 is the splitting ring of the separable polynomial $X^p - X - s_1$ over the weakly uniform ring R ([4, Lemma 1.1]), R_1 is also weakly uniform ([1, Proposition 2.5]). Inductively, R_i are weakly uniform for all $i = 1, 2, \cdots, k$. Especially $M = R_k$ is weakly uniform. This completes the proof of

(iii) ⇒ (ii). Finally we show that (ii) implies (i). We use the same notations as in the proof of Theorem 2. Then T can be taken as a weakly uniform ring by induction hypothesis. Since S is a C-Galois extension of T and C is of order p, then S is also weakly uniform.

REFERENCES

[1] F. DEMEYER: Separable polynomials over a commutative ring, Rocky Mt. J. Math. **2** (1972), 299−310.

[2] G. J. JANUSZ: Separable algebras over commutative rings, Trans. Amer. Math. Soc. **122** (1966), 461−479.

[3] K. KISHIMOTO: On p-extensions of an algebra of characteristic p, J. Algebra, **88** (1984), 173−177.

[4] T. NAGAHARA and A. NAKAJIMA: On cyclic extensions of commutative rings, Math. J. Okayama Univ. **15** (1971), 81−90.

[5] T. NAGAHARA and A. NAKAJIMA: On separable polynomials over a commutative ring IV Math. J. Okayama Univ. **17** (1974), 49−58.

[6] R. S. PIERCE: Mudules over commutative regular rings, Mem. Amer. Math. Soc. No. **70** (1967).

[7] D. J. SALTMAN: Noncrossed product of p-algebras and Galois p-extensions, J. Alg. **52** (1978), 302−314.

[8] O. E. VILLAMAYOR and D. ZELINSKY: Galois theory with infinitely many idempotents, Nagoya Math. J. **35** (1969), 83−93.

[9] E. WITT: Konstruktion von Galoischen Körpern der Charakteristik p zu vorgegebener Gruppe der Ordung p^f, J. für Math. **174** (1936), 237−245.

DEPARTMENT OF MATHEMATICS
OKAYAMA UNIVERSITY

(Received September 18, 1983)