Revista de la
Unión Matemática Argentina
Volumen 24, Número 4, 1969.

ON QUASI-GALOIS EXTENSIONS OF COMMUTATIVE RINGS

by Yasuji Takeuchi

In the ordinary Galois theory of fields the notion of quasi-Galois extension (in the other words, normal extension) plays an important role. Auslander, Goldman, Chase, Harrison, Rosenberg and others have developed Galois theory of commutative rings. On the one hand, Villamayor and Zelinsky studied weakly Galois theory of commutative rings. However the author thinks that in their theory there is no explicit notion corresponding to quasi-Galois extension of fields. Recently he studied on a characterization of the notion of Galois extension of commutative rings {5}. It suggests a possibility for extending the notion of quasi-Galois extension of fields to the case of commutative rings. In this paper we shall try to do it.

In our first section we shall introduce a notion of quasi-Galois extension of commutative rings. In our second section we shall extend to our case theorems concerning to fixed rings in theory of fields. In our final third section we shall study on relations between Galois extensions and quasi-Galois extensions.

In this paper we shall assume that all rings have the identity and are commutative. If R is a commutative ring and if S is a R-algebra $Aut_R(S)$ will denote the group of all automorphisms of S over R. If T is an integral domain, <T> will denote the quotient field of T.

DEFINITION. We begin with introducing a notion of quasi-Galois extension of commutative rings.

DEFINITION 1.1. *Let* R *be a commutative ring and* S *a commutative* R-*algebra that is integral over* R. *Let* G *be the group of all automorphisms of* S *over* R. *Then* S *will be called a quasi-Galois extension of* R *if, for any prime ideal* p *of* R, *the following conditions hold:*

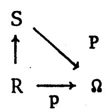
1) *If* P *is a prime ideal of* S *lying over* p, *the quotient field* <S/P> *is a quasi-Galois extension of* <R/p>
2) G *operates transitively on the family of all prime ideals of* S *lying over* p, *i.e. if* P *and* P' *are two prime ideals of* S *lying over* p, *there is* $\sigma \in G$ *such that* $\sigma(P) = P'$.
3) *Any automorphism of* S/P *over* R/p *is canonically induced by an element of* G.

In particular we shall call S *a purely inseparable extension of* R *if, for any prime ideal* p *of* R, *there exists only one prime ideal* P *of* S *lying over* p *and* <S/P> *is a purely inseparable extension of* <R/p>.

REMARK. Let S be a commutative ring and G a finite group of automorphisms of S. If R is the fixed ring of S under G, then S is a quasi-Galois extension of R {c.f. 1, n° 2, theorem 2} .

Let R be a commutative ring. $\tilde{R}$ denotes the afine scheme induced by R. Then there exists a canonical bijective correspondence between the geometric points of $\tilde{R}$ with value in a field K and the homomorphisms of R into K. If p is a geometric point of $\tilde{R}$ with value in K, we shall denote with the same p the corresponding homomor - phism; $R \longrightarrow K$ and call it a geometric point of R with value in K (or simply, a geometric point of R).

If S is a R-algebra, the afine scheme $\tilde{S}$ forms canonically a $\tilde{R}$ - scheme. Let p be any geometric point of $\tilde{R}$. Then $E_p^R(S)$ will denote the set of geometric points of $\tilde{S}$ over p with value in an algebraic closure Ω of <Im(p)> . The set $E_p^R(S)$ can be identified to the set of homomorphisms P of S into Ω such that the diagram



is commutative where the vertical mapping is the structure homomorphism of R-algebra. If σ is a R-automorphism of S, we consider a right operation of σ on $E_p^R(S)$ by $(P\sigma)(x) = P(\sigma(x))$ for $P \in E_p^R(S)$, $x \in S$. Let G be a group of R-automorphisms of S. Then $E_p^R(S)$ consists of the orbits of it's element under G i.e. $E_p^R(S) = \cup_p PG$.

THEOREM 1.2. *Let* R *be a commutative ring and* S *a commutative* R-*algebra that is integral over* R. S *is a quasi-Galois extension of* R *if and only if, for any geometric point* p *of* R, *the set* $E_p^R(S)$ *con - sists of only one orbit of it's element under* G.

In particular, S *is a purely inseparable extension of* R *if and only if, for any geometric point* p *of* R , $E_p^R(S)$ *consists of only one element.*

Proof: The second statement follows easily from the first one. We shall show the first property. The "only if" part is proved similarly as the corollary to theorem 2 of §2 in {1}. The "if" part remains. Let *p* be any prime ideal of R and *P* any prime ideal of S lying over p. If Ω is an algebraic closure of S/P, the inclusion mappings of S/P and of R/p into Ω induce a geometric point P of S and a geometric point p of R, respectively. If $\bar{Q}$ is any R/p-isomorphism of S/P into Ω, $\bar{Q}$ also induces a geometric point Q of S. By the hypothesis there is $\sigma \in G$ such that $P = Q\sigma$ and so $S/P = P(S) = Q(\sigma(S)) = \bar{Q}(S/P)$. Hence $\langle S'/P \rangle$ is a quasi-Galois extension field of $\langle R/p \rangle$. Let Q be any other prime ideal of S lying over p. Since $\langle S/Q \rangle$ is an algebraic extension of $\langle R/p \rangle$, there exists a R/p-isomorphism $\bar{Q}': S/Q \longrightarrow \Omega$. Then $\bar{Q}'$ induces a geometric point Q' of S over p with value in Ω, so that there is $\tau \in G$ such that $P\tau = Q'$. This implies $\tau(P) = Q$. It follows similarly as above that any R/p-automorphism of S/P is canonically induced by an element of G. This completes the proof.

COROLLARY 1.3. *Let* S *be a commutative ring,* G *a group of automorphisms of* S *and* R *the fixed ring of* S *under* G. *If* G *is compact in the finite topology, then* S *is a quasi-Galois extension of* R.

Proof: Let $\{x_1, x_2, \ldots, x_n\}$ be any finite subset of S. The hypothesis implies that the family $\cup_{i=1}^{n} Gx_i$ of the orbits Gx_i forms a finite set. If we put $S_{(x)}$ the subring $R|\cup_{i=1}^{n} Gx_i|$ of S generated by the $\cup_{i=1}^{n} Gx_i$ over R, we obtain $\sigma(S_{(x)}) \subseteq S_{(x)}$ for all $\sigma \in G$. Let $N_{(x)}$ be the set of elements of G which fix every element of $S_{(x)}$. $N_{(x)}$ is a normal subgroup of finite index in G and so the factor group $G/N_{(x)}$ can be regarded canonically as a group of automorphisms of $S_{(x)}$. Then R is the fixed ring of $S_{(x)}$ under $G/N_{(x)}$, so that $S_{(x)}$ is a quasi-Galois extension of R {c.f. the remark of Definition 1.1.}. We consider the family $\{S_{(x)}\}_{(x)}$ consisting of such $S_{(x)}$ for all finite subset $(x) = (x_1, x_2, \ldots, x_n)$ of S. The family $\{S_{(x)}\}_{(x)}$ forms canonically an injective set by the inclusion mappings. Then we obtain that S is canonically isomorphism to $\varinjlim S_{(x)}$.

Let p be any geometric point of R and P, Q two geometric points of S over p. If $g_{(x)}$ is the canonical homomorphism : $S_{(x)} \longrightarrow S$, $Pg_{(x)}$ and $Qg_{(x)}$ are also geometric points of $S_{(x)}$ over p. We consider the sets $G_{(x)} = \{\sigma^1_{(x)}N_{(x)}, \sigma^2_{(x)}N_{(x)}, \ldots, \sigma^{n(x)}_{(x)}N_{(x)} ; \sigma^i_{(x)} \in G, Pg_{(x)}\sigma^i_{(x)} = Qg_{(x)}\}$. $G_{(x)}$ is not empty and $n(x)$ is finite. The family $\{G_{(x)}\}_{(x)}$ forms naturally a projective set, i.e. if $S_{(x)} \subseteq S_{(y)}$, the morphism $\lambda_{(x),(y)}:G_{(y)} \longrightarrow G_{(x)}$ is defined by $\lambda_{(x),(y)}(\sigma^i_{(y)}N_{(y)}) = \sigma^i_{(y)}N_{(x)}$. Then we have $\varprojlim G_{(x)} \neq \emptyset$. We obtain easily that any element of $\varprojlim G_{(x)}$ induces canonically an automorphism τ of S and so $P\tau = Q$.

COROLLARY 1.4. *Let* R *be a commutative ring. If* S *is a quasi-Galois extension of* R *and if* T *is a purely inseparable extension of* R, *then* $S \otimes_R T$ *is a quasi-Galois extension of* R.

Proof: Let p be any geometric point of R and P, Q two geometric points of $S \otimes_R T$ lying over p. If we denote with f the natural homomorphism : $T \longrightarrow S \otimes_R T$, we have $Pf = Qf$ since they are geometric points of T over p. On the other hand if g is the natural homomorphism : $S \longrightarrow S \otimes_R T$, then Pg and Qg are geometric points of S over p, so that $Pg\sigma = Qg$ for some $\sigma \in Aut_R(S)$. This implies $P(\sigma \otimes_R 1) = Q$ where $\sigma \otimes_R 1$ is the R-automorphism of $S \otimes_R T$ induced by σ and the identity automorphism of T.

2. FIXED RINGS.

We begin with an extension of a well-known theorems in theory of fields.

PROPOSITION 2.1. *Let* S *be an overring of* R *that is a finitely generated separable* R-*algebra. If* S *is a purely inseparable extension of* R, *then we have* S = R.

Proof: Since, for any maximal ideal m of R, S_m/mS_m is a separable extension field of R_m/mR_m and is purely inseparable over R_m/mR_m, we have $S_m/mS_m = R_m/mR_m$ and so $S_m = R_m + mS_m$. Hence we obtain S = R.

PROPOSITION 2.2. *Let* R *be a commutative ring and* S *a* R-*algebra. If* S *is a quasi-Galois extension of* R, *then the fixed ring of* S *under the group* G *of all* R-*automorphisms of* S *is a purely inseparable extension of* R.

Proof: Let p be any geometric point of R and P, Q two geometric points of S^G over p. Then P and Q can be extended to geometric points P' and Q' of S, respectively. Since S is a quasi-Galois extension of

R, we have $P'\sigma = Q'$ for $\sigma \in G$ and so $P = Q$. This proves our proposition.

LEMMA 2.3. *Let* R *be a commutative ring without proper idempotent and* S *a* R-*algebra. Assume that* S *is a direct sum of finite number of indecomposable* R-*algebras which are isomorphic to each other as* R-*algebras. If* S *is a finitely generated separable* R-*algebra, then the fixed ring* S^G *is finitely generated as a* R-*module where* $G = \mathrm{Aut}_R(S)$.

Proof: Let $S = S_1 \oplus S_2 \oplus \dots \oplus S_n$ be a decomposition as the assumption. Then each S_i is a Galois extension of the fixed ring T_i of S_i under the group $G_i = \mathrm{Aut}_R(S_i)$. Hence each T_i is finitely generated as a R-module. Now we take any R-isomorphisms $\sigma_1^i : S_1 \longrightarrow S_i$ for $i = 2,3,\dots,n$ and the identity mapping of S_1 as σ_1^1. Set $\sigma_i^j = \sigma_1^j \cdot (\sigma_1^i)^{-1}$ for $i,j = 1,2,\dots,n$. Then σ_i^j is a R-isomorphism: $S_i \longrightarrow S_j$. We shall consider R-automorphisms $\tilde{\sigma}_i^j$ of S such that $\tilde{\sigma}_i^j | S_i = \sigma_i^j$, $\tilde{\sigma}_i^j | S_j = \sigma_j^i$ and $\tilde{\sigma}_i^j | S_k$ = identity mapping of S_k $(k \neq i,j)$ for $i,j = 1,2,\dots,n$. Let H be a subgroup of G generated by the $\tilde{\sigma}_i^j$'s. Then G is a semi-direct product of H and the direct product of the G_i's. Hence we have $S^G = (T_1 \oplus \dots \oplus T_n)^H = \{t + \tilde{\sigma}_1^2(t) + \dots + \tilde{\sigma}_1^n(t);\ t \in T_1\}$, so that S^G is finitely generated as a R-module.

THEOREM 2.4. *Let* R *be a commutative ring and* S *a commutative overring of* R *which is a separable* R-*algebra and is projective as a* R-*module. If* S *is a quasi-Galois extension of* R, *then* R *is the fixed ring of* S *under the group* G *of all* R-*automorphisms of* S.

Proof: First we assume that R has no proper idempotent. S is a direct sum of finite number of indecomposable R-subalgebras. Hence we can write with a form $S = S_1^{n_1} \oplus S_2^{n_2} \oplus \dots \oplus S_r^{n_r}$ where S_i are indecomposable R-algebras such that S_i and S_j $(i \neq j)$ are not isomorphic over R, and $S_i^{n_i}$ denotes a direct sum of n_i copies of S_i. If we put $G_i = \mathrm{Aut}_R(S_i^{n_i})$, then G is isomorphic to the direct product of the G_i's. Let T_i be the fixed ring of $S_i^{n_i}$ under G_i. Then we have $S^G = T_1 \oplus T_2 \oplus \dots \oplus T_r$. Since each T_i is finitely generated as a R-module, S^G is so. Therefore it follows from (2.3) that $S^G = R$. In general R, the same conditions as our theorem are inherited under the fibres S_x and R_x for any point x of the Boolean spectrum of R. Moreover the group of all R_x-automorphisms of S_x is equal to the group G_x of automorphisms of S_x induced by the elements of G. Then we have $R_x = (S_x)^{G_x}$, since R_x has no proper idempotent. Hence we obtain $R = S^G$ {c.f., 7} .

3. RELATIONS BETWEEN QUASI-GALOIS EXTENSIONS AND GALOIS EXTENSIONS.

Let R be a commutative ring, S a R-algebra and G the group of all R-automorphisms of S. For any maximal ideal M of S, as usual, $G_T(M)$ and $G_Z(M)$ (or simply, G_T and G_Z) will denote the inertia group and the decomposition group of M, respectively.

THEOREM 3.1. *Let* R, S *and* G *be as above. Then* S *is a Galois extension of* R *with a Galois group* G *if and only if* S *is a faithful, projective, separable* R*-algebra and is a quasi-Galois extension of* R *such that the inertia group* $G_T(M)$ *of a maximal ideal* M *of* S *lying over any maximal ideal* m *of* R *reduces to the identity.*

Proof: The "only if" part follows from {2}, so that it is sufficient to show the "if" part. It follows from (2.4) that R is the fixed ring of S under G. Let M be any maximal ideal of S. If we put $m = R \cap M$, then S/mS is a finitely generated separable R/m-algebra so that the number of R/m-automorphisms of S/mS is at most finite. Now each element ($\neq$ 1) of G induces a non-trivial R/m-automorphism of S/mS. Hence G is finite. Furthermore the inertia group of any maximal ideal of S reduces to the identity, since all inertia groups of maximal ideals of S lying over a maximal ideal of R are conjugate to each other. This completes the proof.

COROLLARY 3.2. *Let* S *be a Galois extension of* R *with the group of all* R*-automorphisms of* S *as a Galois group. If* R *is a field, then so is* S.

THEOREM 3.3. *Let* S *be a Galois extension of a ring* R *with a Galois group* G *and* T *an intermediate ring of* S *and* R. *Then there exists a normal subgroup* N *of* G *with* $T = S^N$ *if and only if* T *is quasi-Galois and separable over* R.

Proof: The "only if" part is trivial. It is sufficient for proving the "if" part to show $\sigma(T) = T$ for all $\sigma \in G$. Let p and P be the natural homomorphisms : $R \longrightarrow S/M$ and $T \longrightarrow S/M$, respectively, for any maximal ideal M of S. Then p is a geometric point of R and P is also a geometric point of S over p. On the other hand, if f is the natural homomorphism: $\sigma(T) \longrightarrow S/M$, then $f\sigma$ is also a geometric point of T over p. Since T is a quasi-Galois extension of R, we obtain $P\tau = f\sigma$ for some $\tau \in \mathrm{Aut}_R(T)$. Then $P(T) = P\tau(T) = f(\sigma(T))$ and so $T + M = \sigma(T) + M$. Now let m be a maximal ideal of R and $\{M_1, M_2, \ldots, M_n\}$ the set of all maximal ideals of S lying over m. Then $S/M_1 \oplus S/M_2 \oplus \ldots \oplus S/M_n$ is a Galois extension of R/m with a Galois group G. Hence there exists a canonical bijective correspondence between the separable R/m-subalgebra of $S/M_1 \oplus S/M_2 \oplus \ldots \oplus S/M_n$ and the separable R-subalgebra of S. This implies that T and $\sigma(T)$ coincide, since the natural images of T and $\sigma(T)$ in S/mS coincide.

PROPOSITION 3.4. *Let* R *be a commutative ring and* S *a commutative* R-*algebra. If* S *is weakly Galois over* R {*c.f.* 7} , *then* S *is a quasi-Galois extension of* R. *Conversely if* S *is a faithful, projective, separable* R-*algebra and is a quasi-Galois extension of* R, *then* S *is weakly Galois over* R.

Proof: The first statement is trivial {c.f. 7} and the remark of Definition 1.1. Assume that S is a faithful, projective, separable R-algebra and is a quasi-Galois extension of R. Then it is clear that, for any point x of the Boolean spectrum of R, the properties are inherited under the fibre S_x {c.f. 7} . Hence the fibre R_x is the fixed ring of S_x under the group of all R_x-automorphisms of S_x. Then we have $\rho(S_x)G_x = \mathrm{Hom}_{R_x}(S_x, S_x)$ and so $\rho(S)G = \mathrm{Hom}_R(S,S)$ where $\rho: S \longrightarrow \mathrm{Hom}_R(S,S)$ denotes the usual regular representation of S and $G = \mathrm{Aut}_R(S)$. This completes the proof.

REFERENCES

{1} N.Bourbaki. Algèbre commutative, Chap. 5-6, Hermann París 1964.

{2} S.U.Chase, D.K.Harrison and A.Rosenberg. Galois theory and Galois cohomology of commutative rings.Mem.Amer.Math.Soc. N°52 (1965) 15-33.

{3} D.K.Harrison. Abelian extension of commutative rings. ibid.

{4} N.Jacobson. Lecture in abstract algebra, Vol. III, Nostrand New York 1964.

{5} Y.Takeuchi. A note on Galois coverings (to appear).

{6} O.Villamayor and D.Zelinsky. Galois theory for rings with finitely many idempotents, Nagoya Math. J.,Vol.27 (1966) 721-731.

{7} -----------. Galois theory for rings with infinitely many idempotents.

{8} O.Zariski and P.Samuel. Commutative algebra I, II. Nostrand, New York (1960).

Universidad de Buenos Aires.

Osaka Kyoiku University.