J. Math. Soc. Japan
Vol. 41, No. 4, 1989

Cogalois theory for field extensions

By Akira MASUOKA

(Received March 16, 1988)
(Revised July 6, 1988)

Introduction.

Greither and Harrison [0] defined finite cogalois extensions of fields and established for such an extension K/k a 1-1 correspondence ('cogalois correspondence') between the subgroups of $(K^\times/k^\times)_{\mathrm{tor}}$ and *all* the intermediate fields of K/k, where $(K^\times/k^\times)_{\mathrm{tor}}$ denotes the full torsion part of $K^\times/k^\times$. In order to extend the results in [0] to the infinite extensions of fields and to establish the local version of [0], we grasp the notion of a strongly group-graded extensions of fields as follows. Let K/k be a (possibly infinite) extension of fields. $K\otimes K$ has a natural K-coring structure, whose group-likes $\mathrm{Gr}(K\otimes K)$ forms a group isomorphic to $K^\times/k^\times$, where $\otimes=\otimes_k$. For a subgroup $G<K^\times/k^\times=\mathrm{Gr}(K\otimes K)$, the natural K-algebra map

$$\Phi\colon K[G]\longrightarrow K\otimes K$$

is induced from the inclusion $G\subset$the units in $K\otimes K$, where $K[G]$ denotes the group K-algebra. The injectivity of Φ is none other than the left (or right) K-linear independence of G in $K\otimes K$. We say K/k to be *strongly G-graded*, if Φ is bijective. In this case G turns out to be torsion and K/k a radical extension (1.1.3).

In Section 1 we give basic definitions and results on strongly graded extensions, corings and Galois cohomology.

Section 2 is the main part of the paper. For a fixed prime $p\neq$ch. k, K/k is called *p-cogalois* (resp. *cogalois*), if it is a strongly $(K^\times/k^\times)_{p^\infty}$-(resp. $(K^\times/k^\times)_{\mathrm{tor}}$-) graded extension, where $(K^\times/k^\times)_{p^\infty}$ is the p-primary part of $(K^\times/k^\times)_{\mathrm{tor}}$. Such extensions are necessarily algebraically separable. We reproduce Kneser's theorem (2.1.3), which present a criterion for a given $G<(k_s^\times/k^\times)_{\mathrm{tor}}$ be linearly independent, where k_s is the algebraically separable closure of k. We show a Kummer type theorem for p-cogalois extensions (2.2.3) and local and global cogalois correspondence theorems (2.2.4), (2.3.3).

In Section 3 we show a Hopf-Galois correspondence for division k-algebras which generalize the result on strongly graded extensions in Section 1.

Throughout the paper we fix a base field k and write $\otimes=\otimes_k$, ch. k=the

characteristic of k. For a prime $p \neq \mathrm{ch.}\, k$, we denote by ζ_{p^n} ($n \in \boldsymbol{N}$) a primitive p^n-th root of 1 and use the symbol i for ζ_4. Let $(\ )^\times$ denote the units-functor, hence $k^\times = k - \{0\}$. Let $k[G]$ denote the group k-algebra over a group G.

1. Strongly graded extensions of fields.

In this section we fix an extension of fields K/k. We denote by $(K^\times/k^\times)_{\mathrm{tor}}$ the full torsion part of $K^\times/k^\times$, which is denoted by $\mathrm{Cog}(K/k)$ in [**0**].

1.1. Let $\boldsymbol{I}(K/k)$ denote the set of 1-dimensional k-subspaces of K, which forms a group with respect to the multiplication in K. We always identify $\boldsymbol{I}(K/k)$ with $K^\times/k^\times$ via

$$K^\times/k^\times \cong \boldsymbol{I}(K/k), \qquad xk^\times \longmapsto kx. \tag{1.1.1}$$

For an element $g \in K^\times/k^\times = \boldsymbol{I}(K/k)$ we write typically by u_g ($\in K^\times$) a representative of $g \in K^\times/k^\times$, or a k-basis of $g \in \boldsymbol{I}(K/k)$.

1.1.2. Let $G < K^\times/k^\times$ be a subgroup. We have a natural k-linear map

$$\phi\colon \bigoplus_{g\in G} ku_g \longrightarrow K, \tag{1.1.2.a}$$

which is induced from the inclusions $ku_g \hookrightarrow K$. Let $k \subset E \subset K$ be an intermediate field and put $H = G \cap (E^\times/k^\times)$. We can view naturally as $G/H < K^\times/E^\times$. Take a transversal T of H in G. Since $G \cong H \times T$ as sets, (1.1.2.a) can be viewed to decompose as

$$\bigoplus_{h\in H,\, t\in T} k(u_h, u_t) \longrightarrow \bigoplus_{t\in T} Eu_t \longrightarrow K, \tag{1.1.2.b}$$

where the first map is obtained by applying $\bigoplus_{t\in T}(-)$ to the ϕ-map for H and the second is the ϕ-map for G/H.

1.1.3. Let $K = \bigoplus_{g\in G} K_g$ be a G-graded k-algebra with G a certain group, where K_g denotes the g-component. Clearly K_1 is a subfield of K containing k. Moreover, for a normal subgroup $H \lhd G$, $K_H = \bigoplus_{h\in H} K_h$ is a *G-graded subfield of K*, by which we mean a subfield, as well as a G-graded k-subalgebra, of K. This holds true, since K is naturally G/H-graded with K_H the neutral component.

PROPOSITION. *Let K be as above and assume $K_1 = k$. The following are equivalent:*

(a) *K is strongly G-graded in the sense of* [**4**, p. 15], *that is, $K_g K_{g^{-1}} = k$ for all $g \in G$,*

(b) $G = \{g \in G \mid K_g \neq 0\}$,

(c) $\dim_k K_g = 1$ *for all* $g \in G$.

Moreover, if these equivalent conditions hold, then G is an abelian torsion group

and G can be viewed to be a subgroup of $\boldsymbol{I}(K/k)$ via $G\to\boldsymbol{I}(K/k)$, $g\mapsto K_g$, so that K/k is a radical extension.

PROOF. Since $0\neq x\in K_g$ implies $x^{-1}\in K_{g^{-1}}$, we get the equivalence (a)-(c) (see [4, I.4.5, p. 40]). Suppose (a)-(c) hold. By (c) we can view $G<\boldsymbol{I}(K/k)$. If $g\in G$ is torsion-free and $K_g=ku$, then $K_{\langle g\rangle}=\oplus_{n\in\boldsymbol{Z}}ku^n$, a subfield of K, is isomorphic to the group k-algebra $k[\boldsymbol{Z}]$, which is a contradiction. Hence G is torsion. Q. E. D.

In virtue of Proposition we may define as follows.

1.1.4. DEFINITION. Let $G<(K^\times/k^\times)_{\mathrm{tor}}$. The extension K/k is said to be *strongly G-graded*, if the ϕ-map (1.1.2.a) for G is bijective.

1.1.5. PROPOSITION. *Let $G<(K^\times/k^\times)_{\mathrm{tor}}$ and $K=\oplus_{g\in G}ku_g$ be a strongly G-graded extension of k.*

(1) *The subgroups $H<G$ and the G-graded subfields $E\subset K$ correspond bijectively via*

$$H\longmapsto K_H \quad \text{and} \quad E\longmapsto G\cap(E^\times/k^\times),$$

where

$$K_H=\bigoplus_{h\in H}ku_h. \tag{1.1.6}$$

(2) *Let $k\subset E\subset K$ be an intermediate field and put $H=G\cap(E^\times/k^\times)$. Then the following are equivalent:*

(a) *E is G-graded subfield of K,*

(b) *E/k is strongly H-graded,*

(c) *K/E is strongly G/H-graded.*

PROOF. We can prove (1) directly. We show (2). From (1) we obtain the equivalence (a)$\Leftrightarrow$(b). The equivalence (b)$\Leftrightarrow$(c) follows from (1.1.2.b), wherein the composition is bijective in the present case. If (b) holds, then the first map in (1.1.2.b) is bijective, hence so is the second, i. e., (c) holds. Similarly (c)$\Rightarrow$(b). Q. E. D.

1.2. A K-coring is a K-bimodule $\mathcal{C}$ together with K-bimodule maps $\Delta:\mathcal{C}\to\mathcal{C}\otimes_K\mathcal{C}$ and $\varepsilon:\mathcal{C}\to K$ satisfying coassociativity and left and right counit conditions [7]. A group-like in a K-coring $\mathcal{C}$ is an element $g\in\mathcal{C}$ satisfying $\Delta(g)=g\otimes_K g$, $\varepsilon(g)=1$. We denote by $\mathrm{Gr}(\mathcal{C})$ the set of group-likes in $\mathcal{C}$.

The only K-coring we deal with in Sections 1 and 2 is $K\otimes K$, which has the natural K-bimodule structure and the following K-coring structure [7, Example 1.2, p. 393]:

$$\Delta:\ K\otimes K\longrightarrow(K\otimes K)\underset{K}{\otimes}(K\otimes K)=K\otimes K\otimes K,\qquad \Delta(x\otimes y)=x\otimes 1\otimes y,$$

$$\varepsilon\colon K\otimes K \longrightarrow K, \qquad \varepsilon(x\otimes y)=xy.$$

The k-algebra structure on $K\otimes K$ makes $\mathrm{Gr}(K\otimes K)$ a monoid, indeed a group.

PROPOSITION. *There is an isomorphism of groups:*

$$K^\times/k^\times \cong \mathrm{Gr}(K\otimes K), \qquad xk^\times \longmapsto x^{-1}\otimes x. \tag{1.2.1}$$

This is a direct consequence of [8, Lemma 2.5b, b)]. We often identify these groups.

For a subgroup $G<\mathrm{Gr}(K\otimes K)$, the natural K-algebra map

$$\Phi\colon K[G] \longrightarrow K\otimes K \tag{1.2.2}$$

is induced from the inclusion $G\subset(K\otimes K)^\times$, where $K\otimes K$ is viewed as a K-algebra via $K\to K\otimes K$, $x\mapsto x\otimes 1$.

1.3. Let K/k be a (possibly infinite) Galois extension with $\mathcal{G}=\mathrm{Gal}(K/k)$. The natural K-algebra map

$$K\otimes K \xrightarrow{\sim} \mathrm{Map}_c(\mathcal{G}, K), \qquad x\otimes y \longmapsto (\gamma \longmapsto x\gamma(y)) \tag{1.3.1}$$

induces the isomorphism of groups:

$$K^\times/k^\times \cong \mathrm{Gr}(K\otimes K) \cong \mathbf{Z}^1_c(\mathcal{G}, K^\times), \tag{1.3.2}$$

where $\mathrm{Map}_c(\mathcal{G}, K)$ denotes the K-algebra of continuous maps $\mathcal{G}\to K$ and $\mathbf{Z}^1_c(\mathcal{G}, K^\times)$ denotes the group of standard continuous 1-cocycles $\mathcal{G}\to K^\times$. Especially when $\mathcal{G}$ is finite cyclic with a generator $\gamma\in\mathcal{G}$ fixed, (1.3.2) yields Hilbert theorem 90:

$$K^\times/k^\times \xrightarrow{\sim} \mathrm{Ker}(N_{K/k}\colon K^\times\to k^\times), \qquad xk^\times \longmapsto x^{-1}\gamma(x), \tag{1.3.3}$$

where $N_{K/k}$ denotes the norm map (see, e.g., [**1**, 6.8, p. 239]).

REMARK. By taking the torsion part in (1.3.2), we get the isomorphism of groups

$$(K^\times/k^\times)_{\mathrm{tor}} \cong \mathbf{Z}^1_c(\mathcal{G}, \mu(K)),$$

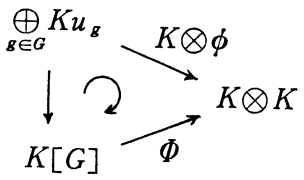
where $\mu(K)$ denotes the group of roots of 1 in K. Hence, if K/k is finite Galois and if $\mu(K)$ is finite, then $(K^\times/k^\times)_{\mathrm{tor}}$ is a finite group. This yields [**0**, Theorem, p. 269].

1.4. Let $G<K^\times/k^\times=\mathrm{Gr}(K\otimes K)$ be a subgroup.

LEMMA AND DEFINITION. *The ϕ-map* (1.1.2.a) *for G is injective (resp. surjective), if and only if the Φ-map* (1.2.2) *for G is injective (resp. surjective).*

When ϕ (or Φ) is injective, equivalently when $\{u_g\}_{g\in G}$ are k-linearly independent in K, we shall say that G is *linearly independent*.

PROOF. The assertion follows from the following commutative diagram:



where the vertical map is the K-linear map determined by $u_g\mapsto u_g\cdot(u_g^{-1}\otimes u_g)$, $g\in G$, which is bijective. Q. E. D.

1.4.1. Let $p\neq$ch. k be a prime and assume that $\zeta_p\notin k$. Then $\langle\zeta_p k^\times\rangle< k(\zeta_p)^\times/k^\times$ is not linearly independent, since the representatives $1, \zeta_p, \zeta_p^2, \cdots, \zeta_p^{p-1}$ are k-linearly dependent. Similarly, if ch. $k\neq 2$ and $i\notin k$, $\langle(1\pm i)k^\times\rangle$ is not linearly independent.

1.4.2. Suppose that K/k is an abelian extension with $\mathcal{G}=\mathrm{Gal}(K/k)$. The isomorphism (1.3.1) preserves the action of $\mathcal{G}$, where $\mathcal{G}$ acts on $K\otimes K$ diagonally and on $\mathrm{Map}_c(\mathcal{G}, K)$ via $(\gamma f)(\gamma')=\gamma(f(\gamma'))$ for $\gamma, \gamma'\in\mathcal{G}$, $f\in\mathrm{Map}_c(\mathcal{G}, K)$. By taking $\mathcal{G}$-invariants in (1.3.2), we get

$$\mathrm{Gr}(K\otimes K)^{\mathcal{G}}\cong\mathrm{Hom}_{\mathrm{c.group}}(\mathcal{G}, k^\times)\subset\mathrm{Hom}_{\mathrm{group}}(\mathcal{G}, K^\times).$$

Since $\mathrm{Hom}_{\mathrm{group}}(\mathcal{G}, K^\times)$ is K-linearly independent by Artin's theorem [**1**, 5.4, Theorem 3, p. 184], it follows that $\mathrm{Gr}(K\otimes K)^{\mathcal{G}}$ is linearly independent. For example, if K/k is an n-Kummer extension for some $n\in\boldsymbol{N}$, then the n-torsion part of $K^\times/k^\times$ is linearly independent, as is well known.

2. Local and global cogalois theory.

Throughout this section we shall make use of the following notation. Denote by k_s the algebraically separable closure of k. Let p be a prime and $n\in\boldsymbol{N}$. Denote by $\mu_n(K)$ the group of n-th roots of 1 in K and put $\mu_{p^\infty}(K)=\bigcup_r\mu_{p^r}(K)$. For $k^\times<M<K^\times$, denote by

$$(M/k^\times)_n,\quad (M/k^\times)_{p^\infty}\quad\text{and}\quad (M/k^\times)_{\mathrm{tor}}$$

the n-torsion part, the p-primary part and the full torsion part of $M/k^\times$, respectively. Hence $(M/k^\times)_{p^\infty}=\bigcup_r(M/k^\times)_{p^r}$ and $(M/k^\times)_{\mathrm{tor}}=\bigoplus_{p:\mathrm{prime}}(M/k^\times)_{p^\infty}$.

2.1. A criterion for linear independence. We shall show a criterion (2.1.3) for a given $G<(k_s^\times/k^\times)_{\mathrm{tor}}$ be linearly independent, which is essentially due to Kneser [**3**]. A closer observation will be made in (2.1.2) in case that $G<(k_s^\times/k^\times)_{p^\infty}$ for some prime $p\neq$ch. k.

2.1.1. LEMMA. *Let p be a prime such that $p\neq$ch. k and let $K=k(x)$ with $x^p\in k^\times-k^{\times p}$.*

(1) *Either if p is odd or if $p=2$ and $i\notin xk^\times$, then $[K: k]=p$ and $(K^\times/k^\times)_{p^\infty}=\langle xk^\times\rangle$.*

(2) *If $p=2$ and $i\in xk^\times$, then $K=k(i)$ and $(K^\times/k^\times)_4=\langle(1\pm i)k^\times\rangle$.*

PROOF. We use Hilbert theorem 90 (1.3.3) repeatedly.

(1) Case $p=2$ and $i\notin xk^\times$. Clearly $[K: k]=2$. Since $(K^\times/k^\times)_2=\langle xk^\times\rangle$ by (1.3.3), $i\notin K-k$ and consequently $i\notin\mathrm{Ker}\, N_{K/k}$, so that $(K^\times/k^\times)_{2^\infty}=\langle xk^\times\rangle$ by (1.3.3).

Case p is odd. Put $E=k(\zeta_p)$ and $L=E(x)=k(\zeta_p, x)$. $(E^\times/k^\times)_p=\langle\zeta_pk^\times\rangle$ by (1.3.3). This and the hypothesis $x^p\notin k^{\times p}$ imply that $x\notin E$. (If $x\in E$, then $x\in\zeta_pk^\times$, so that $x^p\in k^{\times p}$.) Hence L/E is a p-Kummer extension with $[L: E]=p$. Since $[L: K]$ is prime to p, $[K: k]=p$, so that K and E are linearly disjoint over k. Even if $\zeta_{p^2}\in L$, $N_{L/E}(\zeta_{p^2})=\zeta_p\neq 1$. Hence $(L^\times/E^\times)_{p^\infty}=(L^\times/E^\times)_p=\langle xE^\times\rangle$ by (1.3.3). Finally we have

$$(L^\times/E^\times)_{p^\infty}>(K^\times/k^\times)_{p^\infty}=\langle xk^\times\rangle,$$

where '$>$' follows from the linear disjointness of K and E.

(2) is verified easily by using (1.3.3). Q. E. D.

2.1.2. THEOREM. *Fix a prime $p\neq$ch. k and let $k^\times<M<k_s^\times$ with $M/k^\times$ a p-group. If p is odd, assume that $\zeta_p\notin M-k^\times$. If $p=2$, assume that $i\notin M-k^\times$. Then $M/k^\times$ is linearly independent and $(k(M)^\times/k^\times)_{p^\infty}=M/k^\times$.*

PROOF. We can assume that $M/k^\times$ is a finite p-group, since it is a directed union of finite p-groups. We show the claim by induction on $|M/k^\times|$. Let $q=p$ if p is odd, and let $q=4$ if $p=2$. Put $K=k(M)$.

Case $|M/k^\times|=p$. Take an $x\in M$ such that $M/k^\times=\langle xk^\times\rangle$. Since $\zeta_q\notin xk^\times$ (equivalently $x^p\notin k^{\times p}$, if $p\geqq 3$), the claim follows from (2.1.1)(1).

Case $|M/k^\times|\geqq p$. Take $k^\times\leqq N\leqq M$ and put $E=k(N)$. The claim holds for N by the induction hypothesis. Since $(E^\times/k^\times)_{p^\infty}=N/k^\times$, it follows that $N=M\cap E^\times$ and $M/N\cong E^\times M/E^\times$. Assume $\zeta_q\in E^\times M$, then $\zeta_qx\in E^\times$ for some $x\in M$. Since $(E^\times/k^\times)_{p^\infty}=N/k^\times$, $\zeta_qx\in N$, so that $\zeta_q\in M$. This implies $\zeta_q\in k^\times\subset E^\times$ by the hypothesis for M. Hence the induction hypothesis can be applied to $E^\times M/E^\times$ and it follows that $E^\times M/E^\times$ is linearly independent and $(K^\times/E^\times)_{p^\infty}=E^\times M/E^\times$. We have the linear independence of $M/k^\times$ by the argument in (1.1.2.b) and get $(K^\times/k^\times)_{p^\infty}=M/k^\times$ by applying the 5-lemma to the following commutative diagram:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & N/k^\times & \longrightarrow & M/k^\times & \longrightarrow & M/N & \longrightarrow & 1 \quad \text{(exact)} \\ & & \| & & \downarrow & & \| & & \\ 1 & \longrightarrow & (E^\times/k^\times)_{p^\infty} & \longrightarrow & (K^\times/k^\times)_{p^\infty} & \longrightarrow & (K^\times/E^\times)_{p^\infty} & & \text{(exact).} \end{array}$$

Q. E. D.

Here we can reproduce the result by Kneser [3].

2.1.3. THEOREM. *Let* $k^\times<M<k_s^\times$ *with* $M/k^\times$ *torsion. Assume that* ch. $k\neq 2$. *Then* $M/k^\times$ *is linearly independent, if and only if* (a) $\zeta_p\notin M-k^\times$ *for all primes* $p\neq$ch. k *and* (b) $1\pm i\notin M-k^\times$. *When* ch. $k=2$, *the assertion holds true with condition* (b) *deleted.*

PROOF. The 'only if' part is essentially proved in part (c) of the proof of [**0**, Lemma 1.2, p. 285]. See also (1.4.1).

We prove the 'if' part. As in [3], by replacing $M/k^\times$ with $(M/k^\times)_{p^\infty}$, we may assume that $M/k^\times$ is a finite p-group with p a prime$\neq$ch. k. Moreover we can restrict ourselves to the case that $p=2\neq$ch. k and $i\in M-k^\times$, since we are done in (2.1.2) in other cases. Put $E=k(i)\subset k(M)$. The assumption $1\pm i\notin M-k^\times$ and (2.1.1) (2) imply that $M/k^\times\cap E^\times/k^\times=\langle ik^\times\rangle$, which is linearly independent. Since $i\in E$, the quotient group $E^\times M/E^\times=(M/k^\times)/\langle ik^\times\rangle$ is linearly independent by (2.1.2), so that $M/k^\times$ is linearly independent by the argument in (1.1.2.b).

Q. E. D.

2.2. Local cogalois theory. We fix an algebraic extension K/k of fields and a prime $p\neq$ch. k.

Modifying [**0**, Definition, p. 258] we define as follows.

2.2.1. DEFINITION. The extension K/k is called *p-pure*, if

$$\begin{cases}\zeta_p\notin K-k & \text{(case } p \text{ is odd)},\\ i\notin K-k & \text{(case } p=2).\end{cases}$$

PROPOSITION. $(K^\times/k^\times)_{p^\infty}$ *is linearly independent, if and only if* K/k *is p-pure.*

PROOF. Apply (2.1.3) to the inverse image $M\subset K^\times$ of $(K^\times/k^\times)_{p^\infty}$. When $p=2$, note that $i\notin M-k^\times$ if and only if $1\pm i\notin M-k^\times$. Q. E. D.

2.2.2. DEFINITION. Put $G=(K^\times/k^\times)_{p^\infty}$. K/k is *p-coseparable* (resp. *p-cogalois*), if the Φ-map $K[G]\to K\otimes K$ (1.2.2) is surjective (resp. bijective).

It is easily verified that, if K/k is p-coseparable, then K/k is separable and K/E is p-coseparable for any intermediate field $k\subset E\subset K$.

The following are equivalent by definition and the previous proposition: (a) K/k *is p-cogalois*, (b) K/k *is strongly* $(K^\times/k^\times)_{p^\infty}$*-graded in the sense of* (1.1.4), (c) K/k *is p-pure and p-coseparable.*

The following theorem is a direct consequence of (2.1.2).

2.2.3. THEOREM. *Fix a prime* p *such that* $p\neq$ch. k. *Then the subgroups* $M/k^\times<(k_s^\times/k^\times)_{p^\infty}$ *with* $k^\times<M<k_s^\times$ *such that*

$$\begin{cases} \zeta_p \notin M-k^\times & (\textit{case } p \textit{ is odd}) \\ i \notin M-k^\times & (\textit{case } p=2) \end{cases}$$

and the p-cogalois extensions $k\subset E(\subset k_s)$ *correspond bijectively via*

$$M/k^\times \longmapsto k(M) \quad \textit{and} \quad E \longmapsto (E^\times/k^\times)_{p^\infty}.$$

2.2.4. THEOREM. *Let* K/k *be a p-cogalois extension for a prime* $p\neq \mathrm{ch}.\, k$ *and put* $G=(K^\times/k^\times)_{p^\infty}$.

(a) *For any intermediate field* $k\subset E\subset K$, E/k *and* K/E *are both p-cogalois and we have naturally*

$$(K^\times/k^\times)_{p^\infty}/(E^\times/k^\times)_{p^\infty} \cong (K^\times/E^\times)_{p^\infty}.$$

(b) *The subgroups* $H<G$ *and the intermediate fields* $k\subset E\subset K$ *correspond bijectively via*

$$H \longmapsto K_H \ (1.1.6) \quad \textit{and} \quad E \longmapsto (E^\times/k^\times)_{p^\infty}.$$

PROOF. The extension K/k is strongly G-graded. Take any $k\subset E\subset K$. Then K/E is p-cogalois, since it is p-pure and p-coseparable. We have the commutative diagram:

$$\begin{array}{ccc} K[G] & \xrightarrow[\Phi]{\sim} & K\otimes K \\ {\scriptstyle \text{cano.}}\downarrow & \curvearrowright & \downarrow{\scriptstyle \text{proj.}} \\ K[(K^\times/E^\times)_{p^\infty}] & \xrightarrow[\Phi]{\sim} & K\otimes_E K. \end{array}$$

Hence the canonical map $G=(K^\times/k^\times)_{p^\infty}\to(K^\times/E^\times)_{p^\infty}$ is surjective and we have naturally $(K^\times/E^\times)_{p^\infty}\cong G/H$ with $H=(E^\times/k^\times)_{p^\infty}=G\cap E^\times/k^\times$. By (1.1.5)(2), E/k is strongly H-graded, i.e., p-cogalois. Since we have shown any intermediate field is G-graded, we get (b) from (1.1.5)(1). Q.E.D.

2.2.5. Next we observe p-cogalois extensions which are simultaneously Galois.

PROPOSITION (cf. [**0**, Theorem 2.2]). *Let* K/k *be a p-cogalois extension and put* $G=(K^\times/k^\times)_{p^\infty}$.

(1) *Assume that* K/k *is finite with* $n=[K:k]=|G|$ *and let* m *be the exponent of* G. *Then* K/k *is Galois (resp. Kummer, resp. cyclic), if and only if* $\zeta_m\in K$ *(resp.* $\zeta_m\in k$, *resp.* $\zeta_n\in K$ *and* G *is cyclic).*

(2) *Assume that* K/k *is Galois with* $\mathcal{G}=\mathrm{Gal}(K/k)$ *and define the pairing* $\langle\ ,\ \rangle: \mathcal{G}\times G\to\mu_{\mathcal{G}^\infty}(K)$ *by*

$$\langle \gamma, xk^\times \rangle = x^{-1}\gamma(x), \qquad \gamma \in \mathcal{G}, \quad xk^\times \in G .$$

Then we have the isomorphism of groups

(2.2.5.a) $$G \xrightarrow{\sim} \mathbf{Z}^1_c(\mathcal{G}, \mu_{p^\infty}(K)), \qquad g \mapsto \langle ?, g \rangle$$

and the homeomorphism

(2.2.5.b) $$\mathcal{G} \xrightarrow{\sim} \mathrm{Hom}_{\mathrm{group}}(G, K^\times), \qquad \gamma \mapsto \langle \gamma, ? \rangle,$$

where $\mathrm{Hom}_{\mathrm{group}}(G, K^\times)$ *has the open-finite topology. Moreover the subgroups* $H<G$ *and the closed subgroups* $\mathcal{H}<\mathcal{G}$ *correspond bijectively via*

$$H \mapsto H^\perp = \{\gamma \in \mathcal{G} \mid \langle \gamma, H \rangle = \{1\}\} \quad \textit{and} \quad \mathcal{H} \mapsto \mathcal{H}^\perp = \{g \in G \mid \langle \mathcal{H}, g \rangle = \{1\}\}.$$

PROOF. (1) The proof in cases of 'Galois' and 'Kummer' is easy, hence omitted. When K/k is finite Galois, it follows from the 1-1 correspondence in (2) that G is cyclic if and only if $\mathcal{G}=\mathrm{Gal}(K/k)$ is cyclic. Hence K/k is cyclic, if and only if $\zeta_n \in K$ and G is cyclic.

(2) The isomorphism (2.2.5.a) follows from (1.3.2). Taking a finite Galois and p-cogalois sub-extension $k \subset E_\lambda \subset K$ with $G_\lambda = (E^\times/k^\times)_{p^\infty}$, we have

$$\begin{aligned}
&\mathrm{Hom}_{\mathrm{group}}(G_\lambda, K^\times) = \mathrm{Hom}_{\mathrm{group}}(G_\lambda, E_\lambda^\times) \quad \text{(by (1) above)} \\
&\cong \mathrm{Hom}_{E_\lambda\text{-alg}}(E_\lambda[G_\lambda], E_\lambda) \\
&\cong \mathrm{Hom}_{E_\lambda\text{-alg}}(E_\lambda \otimes E_\lambda, E_\lambda) \qquad \text{(since } E_\lambda[G_\lambda] \cong E_\lambda \otimes E_\lambda\text{)} \\
&= \mathrm{Gal}(E_\lambda/k).
\end{aligned}$$

By taking $\varprojlim_\lambda$ we get the homeomorphism (2.2.5.b). We have the last assertion, since the composition

$$\{H<G\} \xleftrightarrow[(2.2.4)(b)]{} \{k \subset E \subset K\} \xleftrightarrow[\text{Galois corresp.}]{} \{\text{closed } \mathcal{H}<\mathcal{G}\}$$

coincides with the correspondence described in (2). Q. E. D.

2.2.6. EXAMPLES. Fix a prime $p \neq \mathrm{ch}.\, k$. Put $q=p$ if $p \geqq 3$, and put $q=4$ if $p=2$.

(1) If $\zeta_q \in k$, then by (2.2.3) the extension corresponding to $(k_s^\times/k^\times)_{p^\infty}$ is a unique maximal p-cogalois extension of k.

(2) (A typical example of a p-cogalois and pro-cyclic Galois extension). $K = \cup_n \boldsymbol{Q}(\zeta_{p^n})$ is a p-cogalois and infinite Galois extension of $k=\boldsymbol{Q}(\zeta_q)$ with

$$\mathrm{Gal}(K/k) \cong \varprojlim \boldsymbol{Z}/p^n\boldsymbol{Z} \quad \text{and} \quad (K^\times/k^\times)_{p^\infty} \cong \varinjlim \boldsymbol{Z}/p^n\boldsymbol{Z}.$$

(3) Suppose K/k is p-cogalois and Galois with $[K: k] \leqq p^3$. By (2.2.5)(1) we can list up the possible $(K^\times/k^\times)_{p^\infty}$ and $\mathrm{Gal}(K/k)$. As a result we get the following: If $p \geqq 3$ and K/k is non-abelian, then K/k is of the form $K=k(\zeta_{p^2}, x)$

with $\zeta_p \in k \not\ni \zeta_{p^2}$, $x^{p^2} \in k^\times - k^{\times p}$ and $x^{p^3} \notin k^{\times p^2}$, and we have

$$(K^\times/k^\times)_{p^\infty} = \boldsymbol{Z}/p^2\boldsymbol{Z} \times \boldsymbol{Z}/p\boldsymbol{Z} \quad \text{and} \quad \mathrm{Gal}(K/k) = \boldsymbol{Z}/p^2\boldsymbol{Z} \rtimes \boldsymbol{Z}/p\boldsymbol{Z}.$$

On the other hand, if $p=2$, K/k is necessarily abelian.

2.3. Global cogalois theory. We fix an algebraic extension K/k of fields.

In our terminology, K/k is *pure* (see [**0**, Definition, p. 258]), if and only if K/k is p-pure for all primes $p \neq \mathrm{ch}.\, k$.

2.3.1. PROPOSITION. *$(K^\times/k^\times)_{\mathrm{tor}}$ is linearly independent, if and only if* (a) *K/k is pure and* (b) *$(K^\times/k^\times)_l = \{1\}$ with $l = \mathrm{ch}.\, k$.*

PROOF. As in part (b) of the proof of [**0**, Lemma 1.2], if $E \supsetneq k$ is a simple purely inseparable extension of exponent 1, then $(E^\times/k^\times)_l$ cannot be linearly independent since $(E^\times/k^\times)_l = E^\times/k^\times$ is infinite. Hence, if $(K^\times/k^\times)_{\mathrm{tor}}$ is linearly independent, (b) holds. It follows from (2.1.3) that, under (b), the linear independence of $(K^\times/k^\times)_{\mathrm{tor}}$ is equivalent to (a). Q. E. D.

We generalize the definitions in [**0**, p. 257] as follows:

2.3.2. DEFINITION. Put $G = (K^\times/k^\times)_{\mathrm{tor}}$. K/k is *coseparable* (resp. *cogalois*), if $\Phi : K[G] \to K \otimes K$ (1.2.2) is surjective (resp. bijective).

The following theorem is a generalization of Greither and Harrison [**0**, Theorems 1.5, 1.6, pp. 260-261] to the infinite extensions of fields.

2.3.3. THEOREM. *Let K/k be an algebraic extension of a possibly infinite degree.*

(1) *The following are equivalent:*

(a) *K/k is cogalois,*

(b) *K/k is pure, coseparable and separable,*

(c) *K/k is pure, coseparable and $(K^\times/k^\times)_l = \{1\}$ with $l = \mathrm{ch}.\, k$.*

(2) *Let K/k be cogalois and put $G = (K^\times/k^\times)_{\mathrm{tor}}$.*

(a) *For any intermediate field $k \subset E \subset K$, E/k and K/E are both cogalois and we have naturally*

$$(K^\times/k^\times)_{\mathrm{tor}}/(E^\times/k^\times)_{\mathrm{tor}} \cong (K^\times/E^\times)_{\mathrm{tor}}.$$

(b) *The subgroups $H < G$ and the intermediate fields $k \subset E \subset K$ correspond bijectively via*

$$H \longmapsto K_H \ (1.1.6) \quad \text{and} \quad E \longmapsto (E^\times/k^\times)_{\mathrm{tor}}.$$

PROOF. Part (1) is a direct consequence of (2.3.1).

(2) The proof of (2.2.4) goes word for word. Q. E. D.

Assume that K/k is cogalois. For every prime $p \neq \mathrm{ch}.\, k$, the sub-extension

K_p/k which corresponds to $(K^\times/k^\times)_{p^\infty}$ in (2.3.3)(2.b) is a p-cogalois extension and we have $K=\otimes_p K_p$.

REMARK. Even if M, $k^\times<M<k_s^\times$, satisfies the condition that $\zeta_p\notin M-k^\times$ for primes $p\neq$ ch. k (and for $p=4$ if ch. $k\neq 2$), $k(M)/k$ is not necessarily pure. Hence in the global case the correspondence $M\mapsto k(M)$ is not injective. For example, when we put

$$k=\boldsymbol{Q},\qquad M_1=\langle\sqrt{-3},\ \sqrt[3]{2},\ k^\times\rangle,\qquad M_2=\langle\sqrt{-3},\ \sqrt[3]{2}\zeta_3,\ k^\times\rangle,$$

we have $M_1\neq M_2$ and $k(M_1)=k(M_2)$. On the other hand there exists the global version of (2.2.5).

2.3.4. The correspondence in (2.2.4)(b) yields a 1-1 *cogalois correspondence* for a certain class of Galois extensions which involves Kummer extensions.

PROPOSITION. *Let $k^\times<M<k_s^\times$ with $M/k^\times$ torsion. Assume that, for every prime p satisfying $(M/k^\times)_p\neq\{1\}$, (a) $\zeta_p\in k$ and (b) $(M/k^\times)_{p^{n-1}}\subsetneqq(M/k^\times)_{p^n}$ for any $2\leqq n\in\boldsymbol{N}$ implies $\zeta_{p^n}\in M$. If $(M/k^\times)_2\subsetneqq(M/k^\times)_4$, assume in addition that $i\in k$. Then there is a 1-1 correspondence between the intermediate groups $k^\times<N<M$ and the intermediate fields $k\subset E\subset k(M)$, which is given by $N\mapsto k(N)$.*

PROOF. The assumptions assure that the extension K_p/k corresponding to $(M/k^\times)_{p^\infty}$ is 'Galois and p-cogalois' or 2-Kummer. Since $k(M)=\otimes K_p$ and any intermediate field of $k(M)/k$ is a composition of those of K_p/k's, the assertion follows from (2.2.4)(b). Q. E. D.

Greither and Harrison [**0**, Theorem 2.3] follow directly from this result. The assumption ch. $k=0$ is not necessary.

COROLLARY ([**0**, Theorem 2.3]). *Let*

$$f(T)=(T^{n_1}-a_1)(T^{n_2}-a_2)\cdots(T^{n_r}-a_r)$$

be a polynomial with $a_j\in k^\times$ and $n_j\in\boldsymbol{N}$ such that every n_j is not divided by ch. k, *and let K be the splitting field of $f(T)$ over k. Assume that $\zeta_p\in k$ for every odd prime p dividing some n_j. If 4 divides some n_j, assume in addition that $i\in k$. Then any intermediate field of K/k is generated over k by monomials in roots of $f(T)$.*

PROOF. Apply Proposition to $M=\langle\sqrt[n_1]{a_1},\ \sqrt[n_2]{a_2},\ \cdots,\ \sqrt[n_r]{a_r},\ \zeta_m,\ k^\times\rangle$ and $K=k(M)$, where $m=$the least common multiple of $\{n_j\}$. Q. E. D.

3. A Hopf-Galois correspondence for division algebras.

We generalize (1.1.5) to a Hopf-Galois extension. In this section, K denotes a division k-algebra. We use the notation and terminology of [**6**] for the theory of coalgebras. Especially, a Hopf algebra means a bialgebra with the antipode ([**6**, Definition, p. 71]).

M. Takeuchi [**8**] develops a certain Galois theory of the Picard-Vessiot type in the context of C-ferential fields, with C a cocommutative coalgebra. As is pointed out in [**9**], the theory goes parallel for J-comodule k-fields L/E, with J a commutative k-bialgebra. We go partially after the *comodule fields-Picard-Vessiot theory*, but we deal with division k-algebras.

Let (J, Δ, ε) be a k-bialgebra. For a right J-comodule V, we denote its structure by $\rho=\rho_V: V\to V\otimes J$ and its invariants by $V_0=\{v\in V \mid \rho(v)=v\otimes 1\}$.

3.1. Let J be a k-bialgebra and K a right J-comodule division k-algebra. It is easy to see that K_0 is a division subalgebra of K.

3.1.1. Note that, though K is non-commutative, K-corings are defined in an obvious way and $K\otimes K$ has the natural K-coring structure as in (1.2) (see [**7**, 1.1-1.2]). View $K\otimes K$ as a right J-comodule via

$$\text{(3.1.1.a)}\quad K\otimes K \xrightarrow{\rho\otimes\rho} K\otimes J\otimes K\otimes J \xrightarrow{K\otimes tw\otimes J} K\otimes K\otimes J\otimes J \xrightarrow{K\otimes K\otimes m} K\otimes K\otimes J,$$

where tw denotes the twist map and m denotes the multiplication. We mean by a *quotient J-comodule K-coring* a quotient object as a J-comodule and K-coring. $K\otimes_{K_0}K$ is a quotient J-comodule K-coring of $K\otimes K$. Similarly to [**8**, Theorem 2.0], we can prove the following from [**7**, Theorem 2.1].

LEMMA. *There is a* 1-1 *correspondence between the J-comodule division k-subalgebras $E\subset K$ which contain K_0 and the quotient J-comodule K-corings of $K\otimes_{K_0}K$, which is given by $E\mapsto K\otimes_E K$.*

3.1.2. LEMMA. *Let V be a left K-space and simultaneously a right J-comodule such that $\rho_V: V\to V\otimes J$ is left K-linear, where $V\otimes J$ is viewed as a left K-space through ρ_K, i.e.,*

$$x.(v\otimes a)=\rho_K(x)(v\otimes a)$$

for $x\in K$, $v\in V$, $a\in J$. Then

$$\sigma: K\otimes_{K_0}V_0\longrightarrow V, \qquad \sigma(x\otimes v)=xv$$

is injective.

PROOF. Suppose $\operatorname{Ker}\sigma\neq 0$. Choose a non-zero element $\omega=\sum_{j=1}^{r}x_j\otimes v_j\in\operatorname{Ker}\sigma$ with r minimal. Clearly $r\neq 1$. We can assume $x_1=1$. By the minimality of

r, $\{v_j\}$ are left K_0-linearly independent and $x_j \notin K_0$ for $j \geqq 2$. Since $x_r \notin K_0$, we can choose a k-linear map $f: J \to k$ such that $f(1)=1$ and $y_r \neq x_r$, where y_j is the image of x_j under the composition $K \xrightarrow[\rho]{} K \otimes J \xrightarrow[K\otimes f]{} K$. Note $y_1=1$. Then $\omega' = \sum_1^r y_j \otimes v_j \in \operatorname{Ker}\sigma$, since $0=(V\otimes f)\rho_V(\sum x_j v_j)=\sum y_j v_j$. We have

$$0 \neq \omega - \omega' = \sum_{j=2}^{r} (x_j - y_j) \otimes v_j \in \operatorname{Ker}\sigma ,$$

a contradiction to the minimality of r. Hence $\operatorname{Ker}\sigma = 0$. Q. E. D.

We view $K \otimes J$ as a K-bimodule via

$$x.(z \otimes a).y = (xz \otimes a)\rho_K(y)$$

for $x, y \in K$ and $z \otimes a \in K \otimes J$. Then $K \otimes J$ is a K-coring with the following structure:

$$(3.1.3) \qquad K \otimes J \xrightarrow[K\otimes\Delta]{} K \otimes J \otimes J \cong (K \otimes J) \underset{K}{\otimes} (K \otimes J), \qquad K \otimes J \xrightarrow[K\otimes\varepsilon]{} K \otimes k = K .$$

We also view $K \otimes J$ as a right J-comodule via

$$(3.1.4) \qquad K \otimes J \xrightarrow{\rho\otimes J} K \otimes J \otimes J \xrightarrow{K\otimes t w} (K \otimes J) \otimes J .$$

Following [5] we call a coideal $\mathfrak{a} \subset J$ a *right bi-ideal*, if $\mathfrak{a}$ is a right ideal of J.

3.1.5. PROPOSITION. *Assume*

$$\beta : K \otimes K \longrightarrow K \otimes J , \qquad \beta(x \otimes y) = (x \otimes 1)\rho(y)$$

is bijective. Then any quotient J-comodule K-coring of $K \otimes J$ is of the form $K \otimes (J/\mathfrak{a})$ for some right bi-ideal $\mathfrak{a} \subset J$.

PROOF. Clearly $(K \otimes J)_0 = J$. Note that $K_0 = k$, since

$$K_0 = \operatorname{Ker}(K \underset{x\mapsto x\otimes 1}{\overset{\rho}{\rightrightarrows}} K \otimes J) = \operatorname{Ker}(K \underset{x\mapsto x\otimes 1}{\overset{x\mapsto 1\otimes x}{\rightrightarrows}} K \otimes K) = k .$$

Let $w: K \otimes J \to W$ be a quotient map. Since w decomposes as $K \otimes J \xrightarrow{K\otimes w_0} K \otimes W_0 \xrightarrow{\sigma} W$, σ is surjective, hence bijective by (3.1.2). It follows that $W = K \otimes (J/\mathfrak{a})$ for some k-subspace $\mathfrak{a} \subset J$. Since W is K-bimodule quotient and β is bijective, we have $(k \otimes \mathfrak{a}) \cdot (K \otimes J) \subset K \otimes \mathfrak{a}$. Hence $\mathfrak{a}$ is a right ideal of J. Similarly, since W is K-coring quotient, $\mathfrak{a}$ is a coideal of J, so that $\mathfrak{a}$ is a right bi-ideal of J.

Q. E. D.

3.2. Let J be a k-bialgebra. We call division k-algebras $K \supset F$ a *J-Galois extension*, if K is a right J-comodule k-algebra, if $K_0 = F$ and if

$$\beta\colon K\underset{F}{\otimes}K\longrightarrow K\otimes J,\qquad \beta(x\underset{F}{\otimes}y)=(x\otimes 1)\rho_K(y)$$

is bijective.

3.2.1. THEOREM. *Let J be a cocommutative Hopf k-algebra and suppose that a division k-algebra K is a J-Galois extension over k.*

(1) *There is a* 1-1 *correspondence between the right bi-ideals $\mathfrak{a}\subset J$ and the J-comodule division k-subalgebras $E\subset K$. The correspondence is given by*

$$\mathfrak{a}\longmapsto\{x\in K\mid \rho_K(x)\equiv x\otimes 1 \bmod K\otimes\mathfrak{a}\}.$$

(2) *Suppose that $\mathfrak{a}\mapsto E$ in* (1).

(a) *The β-map*

$$\beta\colon K\otimes K\xrightarrow{\sim} K\otimes J,\qquad \beta(x\otimes y)=(x\otimes 1)\rho(y) \tag{3.2.2}$$

induces the isomorphism

$$K\underset{E}{\otimes}K\xrightarrow{\sim}K\otimes(J/\mathfrak{a}).$$

Hence, if $\mathfrak{a}$ is a bi-ideal of J, then K/E is viewed naturally as a $J/\mathfrak{a}$-Galois extension.

(b) *E/k is viewed naturally as a J_1-Galois extension, where $J_1=\{x\in J\mid \Delta(x)\equiv x\otimes 1 \bmod J\otimes\mathfrak{a}\}$.*

PROOF. Since J has the bijective antipode, it follows from the same argument as in [2, Proposition 1.2] that the β-map (3.2.2) is bijective if and only if

$$\beta'\colon K\otimes K\longrightarrow K\otimes J,\qquad \beta'(x\otimes y)=\rho(x)(y\otimes 1) \tag{3.2.3}$$

is bijective.

(1) Since J is cocommutative, the β-map (3.2.2) is an isomorphism of J-comodules and K-corings with respect to the structures described in (1.2), (3.1.1.a), (3.1.3) and (3.1.4). We know from (3.1.1) and (3.1.5) that there is a 1-1 correspondence between the two sets. The correspondence is realized as described above, since, if the isomorphism $K\otimes_E K\simeq K\otimes(J/\mathfrak{a})$ is induced from β, it should hold that

$$E=\mathrm{Ker}\Big(K\underset{x\mapsto x\otimes 1}{\overset{x\mapsto 1\otimes x}{\rightrightarrows}}K\underset{E}{\otimes}K\Big)=\mathrm{Ker}\Big(K\underset{x\mapsto x\otimes 1}{\overset{\rho}{\rightrightarrows}}K\otimes(J/\mathfrak{a})\Big).$$

(2) Suppose $\mathfrak{a}\mapsto E$. We have proved (a) in the proof of (1). Since (3.2.3) is an isomorphism of $J/\mathfrak{a}$-comodules with respect to the structures

$$K\otimes K\xrightarrow{\rho\otimes K}K\otimes J\otimes K\xrightarrow{K\otimes tw}K\otimes K\otimes J\xrightarrow{K\otimes K\otimes\mathrm{proj}}K\otimes K\otimes(J/\mathfrak{a}),$$

$$K\otimes J \xrightarrow{K\otimes\Delta} K\otimes J\otimes J \xrightarrow{K\otimes J\otimes\mathrm{proj}} K\otimes J\otimes(J/\mathfrak{a}),$$

we get $E\otimes K\cong K\otimes J_1$ through β' by taking invariants. Noting that the structure $K\to K\otimes(J/\mathfrak{a})$ is left E-linear, we know that the previous isomorphism preserves the coaction of $J/\mathfrak{a}$ induced from the factor K in each side. By taking invariants we get $E\otimes E\cong E\otimes J_1$ through β'. Since J_1 is a Hopf subalgebra of J by [**5**, Corollary 3.4], it follows from the beginning remark that $E\otimes E\cong E\otimes J_1$ through β. Hence E/k is J_1-Galois. Q.E.D.

Let K/k be a strongly G-graded extension (1.1.3) of fields with $G<(K^\times/k^\times)_{\mathrm{tor}}$. Then K/k is $k[G]$-Galois with the structure $K\xrightarrow[x\mapsto 1\otimes x]{} K\otimes K\underset{\phi^{-1}}{\simeq} K\otimes k[G]$. Hence Theorem (3.2.1) is a generalization of Proposition (1.1.5).

3.2.5. REMARK. The following fact, proved in [**10**], justifies the assumption in (3.2.1) that J is not a bialgebra but a Hopf algebra: *Let J be a cocommutative k-bialgebra. Suppose that there exists such a J-comodule k-algebra R whose β-map*

$$\beta\colon R\otimes R\longrightarrow R\otimes J,\qquad \beta(x\otimes y)=(x\otimes 1)\rho(y)$$

is bijective and which satisfies the condition that $R^n\cong R^m$ for any $n, m\in\boldsymbol{N}$ implies $n=m$, where R^n means the direct sum of n copies of the left (or right) R-module R. Then J is a Hopf algebra.

ACKNOWLEDGEMENT. I would like to thank Professors M. Takeuchi and Y. Doi for suggesting several points to be improved.

References

[0] C. Greither and D.K. Harrison, A Galois correspondence for radical extensions of fields, J. Pure Appl. Algebra, **43** (1986), 257-270.
[1] P.M. Cohn, Algebra, vol. 2, John Wiley, London-New York-Sydney-Toronto, 1977.
[2] H.F. Kreimer and M. Takeuchi, Hopf algebras and Galois extensions of an algebra, Indiana Univ. Math. J., **30** (1981), 675-692.
[3] M. Kneser, Lineare Abhängigkeit von Wurzeln, Acta. Arith., **XXVI** (1975), 307-308.
[4] C. Năstăsescu and F. Van Oystaeyen, Graded Ring Theory, North-Holland, Amsterdam-New York-Oxford, 1982.
[5] K. Newman, A correspondence between bi-ideals and sub-Hopf algebras in cocommutative Hopf algebras, J. Algebra, **36** (1975), 1-15.
[6] M.E. Sweedler, Hopf algebras, Benjamin, New York, 1969.
[7] M.E. Sweedler, The predual theorem to the Jacobson-Bourbaki theorem, Trans. Amer. Math. Soc., **213** (1975), 391-406.

[8] M. Takeuchi, A Hopf algebraic approach to the Picard-Vessoiot theory, J. Algebra, to appear.
[9] M. Takeuchi, A private communication, January 1987.
[10] A. Masuoka, Corings and invertible bimodules, Tsukuba J. Math., to appear.

Akira MASUOKA
Department of Mathematics
University of Tsukuba
Tsukuba-city, Ibaraki 305
Japan