Osaka Mathematical Journal
Vol. 8, No. 1, June, 1956.

On Compact Galois Groups of Division Rings

By Nobuo NOBUSAWA

On the subject of general non-commutative Galois theory, the present author has proved the existence of a fundamental correspondence between topologically closed regular subgroups and subrings for Galois division ring extensions with locally finite Galois groups,—in this case the groups are compact.[1] The main object of this paper is to give a necessary and sufficient condition for such compact Galois groups. In §1 it will be proved that a locally finite regular automorphism group is essentially outer, that is, can not contain but a finite number of inner automorphisms. Conversely we shall show in §2 that an essentially outer regular automorphism group is necessarily locally finite when the division ring extension is algebraic. At the same time, an extension theorem and a normality theorem will be proved for the Galois extensions in [7]. And lastly in §3 it will be proved that in the Galois extensions under the same assumptions any finite extensions are simply generated.

§1. Locally finite automorphism groups.

Let $\mathfrak{G}$ be a group of automorphisms of a division ring P. All the $\mathfrak{G}$–invariant elements of P form a subring Φ of P; in this situation we say that $\mathfrak{G}$ is an automorphism group of P/Φ.

DEFINITION. $\mathfrak{G}$ is said to be *locally finite* when each element of P is mapped by $\mathfrak{G}$ to at most a finite number of elements.

It is clear that, if there exists an automorphism group of P/Φ which is locally finite, then P is locally (left) finite over Φ, that is, any subring generated by Φ and a finite number of elements of P has a finite (left) rank over Φ. For, such a subring is always considered to be contained in a ring which has a finite automorphism group over Φ and the ring with a finite automorphism group over Φ has a finite rank over Φ.[2]

1) See [7].

2) Its rank is not greater than the number of elements of the automorphism group. See [3].

The regularization $\mathfrak{G}^*$ of a given automorphism group $\mathfrak{G}$ is defined thus: if $\mathfrak{G}$ is an automorphism group of P/Φ, we consider all the inner automorphisms of P leaving each element of Φ invariant, that is, the inner automorphisms induced by all the elements of $V(\Phi)$[3]; $\mathfrak{G}^*$ is the group generated by these inner automorphisms and $\mathfrak{G}$. We say $\mathfrak{G}$ is a regular group if $\mathfrak{G}^*=\mathfrak{G}$.

The main idea of the proof of the next Lemma is due to D. Zelinsky who kindly permitted me to cite it here.

Lemma 1. *Let $\mathfrak{G}$ be a regular group of* P/Φ *which consists only of inner automorphisms (hence of all the inner automorphisms induced by the element of* $V(\Phi)$*). If there exists an element of* P *that is moved really by $\mathfrak{G}$ but to at most a finite number of elements, then $V(\Phi)$ is a finite field, that is, $\mathfrak{G}$ is a finite abelian group.*

Proof. Let σ be the element as mentioned in the Lemma. Then there exists such an element $\rho(\neq 0)$ in $V(\Phi)$ that $\rho\sigma\rho^{-1}\neq\sigma$ by the assumption.

1°. First we shall show that $V(\sigma, \Phi)$ is a finite field where $V(\sigma, \Phi)$ is the centralizer of the ring generated by σ and Φ. For any element τ of $V(\sigma, \Phi)$ we denote by I_τ the inner automorphism induced by $1+\rho\tau$. Since $1+\rho\tau\in V(\Phi)$, I_τ is contained in $\mathfrak{G}$. Now it will be shown that, if $\tau\neq\tau'$ $(\tau, \tau'\in V(\sigma, \Phi))$, then $\sigma I_\tau\neq\sigma I_{\tau'}$.[4] For, assume $\sigma I_\tau=\sigma I_{\tau'}$. Then $(1+\rho\tau)\sigma(1+\rho\tau)^{-1}=(1+\rho\tau')\sigma(1+\rho\tau')^{-1}$ and hence $(1+\rho\tau')^{-1}(1+\rho\tau)\sigma((1+\rho\tau')^{-1}(1+\rho\tau))^{-1}=\sigma$, that is, $(1+\rho\tau')^{-1}(1+\rho\tau)=\tau''\in V(\sigma, \Phi)$. This implies that $\rho(\tau-\tau'\tau'')=\tau''-1\in V(\sigma, \Phi)$. Since ρ is not contained in $V(\sigma, \Phi)$, we have $\tau-\tau'\tau''=\tau''-1=0$, that is, $\tau=\tau'$, which is a contradiction. Considering then that $\{\sigma I_\tau \mid \tau\in V(\sigma, \Phi)\}$ must be finite by assumption, we get the result that $V(\sigma, \Phi)$ is a finite set. Since it is a division ring, it is a finite field.

2°. Next we shall show that $[V(\Phi): V(\sigma, \Phi)]_l<\infty$. Let $\alpha_1^{-1}\sigma\alpha_1(=\sigma)$, $\alpha_2^{-1}\sigma\alpha_2, \cdots, \alpha_n^{-1}\sigma\alpha_n$ be all the different images of σ by $\mathfrak{G}$ where α_i are elements of $V(\Phi)$. Now for any element ξ of $V(\Phi)$, we have $\xi^{-1}\sigma\xi=\alpha_i^{-1}\sigma\alpha_i$ for some element α_i; that is, $\xi\alpha_i^{-1}\in V(\sigma, \Phi)$ and hence $\xi\in V(\sigma, \Phi)\alpha_i$. This implies that $\alpha_1, \alpha_2, \cdots, \alpha_n$ form a (not necessarily independent) $V(\sigma, \Phi)$-basis of $V(\Phi)$. Thus we have $[V(\Phi): V(\sigma, \Phi)]_l<\infty$.

By 1° and 2°, $V(\Phi)$ is a finite field.

---

3) $V(\Phi)$ implies the centralizer of Φ in P.

4) All our operators will be written on the right. As a result of this convention, a product st of operators means the composite obtained by performing first s, then t.

The proof of the next Theorem on a necessary condition for locally finiteness is now quite easy by Lemma 1.

Theorem 1.[5] *Let* $\mathfrak{G}$ *be a regular automorphism group of* P/Φ. *If* $\mathfrak{G}$ *is locally finite, then* $\mathfrak{G}$ *contains at most a finite number of inner automorphisms of* P.

Proof. If $\mathfrak{H}$ is the set of all the inner automorphisms contained in $\mathfrak{G}$, then $\mathfrak{H}$ is a locally finite regular automorphism group of P/Ψ where Ψ is the subring of all the $\mathfrak{H}$-invariant elements of P. If $P \neq \Psi$, then $\mathfrak{H}$ is a finite group by Lemma 1. And if $P = \Psi$, then $\mathfrak{H}$ consists only of the identity automorphism.

We insert here an example of finite regular automorphism groups which consist only of inner automorphisms.

Let F be a finite field consisting of p elements (p is a prime number) and K an infinite algebraic extension of F. We construct a non-commutative polynomial ring $K[x]$ where x is an indeterminate and the multiplication of x with an element k of K is defined so that $xk = k^p x$ ($k \in K$). Now we can make the quotient division ring $K(x)$ of $K[x]$. The center of $K(x)$ is F. Let L be any finite extension of F contained in K. All the inner automorphisms induced by the elements of L make a finite regular automorphism group which consists only of inner automorphisms.

REMARK. From Lemma 1, it is clear that if the characteristic of P is 0 then $\mathfrak{G}$ is an outer automorphism group, that is, $\mathfrak{G}$ contains no inner automorphism except the identity automorphism.

§ 2. Essentially outer automorphism groups and Galois theory.

It has been shown in § 1 that a locally finite regular automorphism group contains only a finite number of inner automorphisms, but it will be proved that conversely a regular automorphism group of P/Φ which contains only a finite number of inner automorphisms is necessarily locally finite if P is (left) algebraic over Φ.

Let Σ be a subring of P containing Φ. Σ is considered as a Φ_l-module where Φ_l signifies the ring of operators induced by left multiplications of the elements of Φ. The most important role is played by $\mathfrak{M}(\Sigma)$ which we define as the set of all the Φ_l-homomorphisms of Φ_l-module Σ into P. $\mathfrak{M}(\Sigma)$ is then a Σ_r (left)-P_r (right) two-sided module.

5) The same result has been first given by T. Nagahara and H. Tominaga. See [5].

Lemma 2. *If* $[\Sigma:\Phi]_l = n < \infty$, *then* $[\mathfrak{M}(\Sigma):\mathrm{P}_r]_r = n$.

Proof. Let $\xi_1, \xi_2, \cdots, \xi_n$ be an independent Φ_l-basis of Σ. Any element of $\mathfrak{M}(\Sigma)$ is then uniquely determined by its restriction to ξ_i. If e_i are the elements of $\mathfrak{M}(\Sigma)$ such that $\xi_i e_i = 1$ and $\xi_j e_i = 0$ $(j \neq 1)$, then $e_1, e_2, \cdots, e_n$ form an independent P_r-right basis of $\mathfrak{M}(\Sigma)$.

Let $\mathfrak{G}$ be an automorphism group of P/Φ. We denote by $\mathfrak{G}_\Sigma$ the restrictions of $\mathfrak{G}$ to Σ and by S_Σ $(S \in \mathfrak{G})$ the restriction of S to Σ. It is clear that $\mathfrak{G}_\Sigma \mathrm{P}_r$ is a $\Sigma_r - \mathrm{P}_r$ two-sided submodule of $\mathfrak{M}(\Sigma)$ and $S_\Sigma \mathrm{P}_r$ is an irreducible $\Sigma_r - \mathrm{P}_r$ two-sided submodule of $\mathfrak{M}(\Sigma)$.

Lemma 3. *Let* $\mathfrak{N}$ *be an irreducible* $\Sigma_r - \mathrm{P}_r$ *two-sided submodule of* $\mathfrak{M}(\Sigma)$ *which is isomorphic to* $S_\Sigma \mathrm{P}_r$. *If an element* s *of* $\mathfrak{N}$ *corresponds to* S_Σ *in this isomorphism, then* $s = S_\Sigma(1 \cdot s)_l$.

Proof. For any element σ of Σ, $\sigma_r s$ corresponds to $\sigma_r S_\Sigma$ in this isomorphism, but $\sigma_r S_\Sigma = S_\Sigma(\sigma \cdot S_\Sigma)$. On the other hand $s(\sigma \cdot S_\Sigma)$ corresponds to $S_\Sigma(\sigma \cdot S_\Sigma)$, and hence $\sigma_r s = s(\sigma \cdot S_\Sigma)$. Then, $\sigma \cdot s = 1 \cdot \sigma_r s = 1 \cdot s(\sigma \cdot S_\Sigma)$ $= \sigma \cdot S_\Sigma(1 \cdot s)_l$. Hences $s = S_\Sigma(1 \cdot s)_l$.

DEFINITION. P is said to be (left) *algebraic* over Φ if any subring generated by Φ and an element of P has a finite (left) rank over Φ.

Theorem 2. *Let* $\mathfrak{G}$ *be a regular automorphism group of* P/Φ *where* P *is algebraic over* Φ. *If* $\mathfrak{G}$ *contains only a finite number of inner automorphisms, then* $\mathfrak{G}$ *is locally finite.*

Proof. It will suffice to show that, for any subring Σ of P which contains Φ and has a finite rank over Φ, $\mathfrak{G}_\Sigma$ is a finite set, because P is algebraic over Φ and each element of P is contained in such a subring Σ.

By Lemma 2 we have $[\mathfrak{G}_\Sigma \mathrm{P}_r : \mathrm{P}_r]_r \leq [\mathfrak{M}(\Sigma):\mathrm{P}_r]_r = [\Sigma:\Phi]_l < \infty$ and hence there do not exist infinitely many irreducible $\Sigma_r - \mathrm{P}_r$ two-sided modules which are not isomorphic with each other. On the other hand, let T and S be two elements of $\mathfrak{G}$ such that $T_\Sigma \mathrm{P}_r$ is isomorphic to $S_\Sigma \mathrm{P}_r$. If $T_\Sigma \rho_r$ $(\rho \in \mathrm{P})$ corresponds in this isomorphism to S_Σ, then by Lemma 3 $T_\Sigma \rho_r = S_\Sigma(1 \cdot T_\Sigma \rho_r)_l = S_\Sigma \rho_l$, that is, $T_\Sigma = S_\Sigma I$ where $I = \rho_l \rho_r^{-1} \in \mathfrak{G}$. But the inner automorphisms in $\mathfrak{G}$ are finite in number, and this implies that $\mathfrak{G}_\Sigma$ is finite.

Lemma 4. *If* $\mathfrak{G}$ *is a locally finite regular automorphism group of* P/Φ, *then* $\mathfrak{M}(\Sigma) = \mathfrak{G}_\Sigma \mathrm{P}_r$ *for any subring* Σ *which has a finite rank over* Φ.

Proof. Σ is imbedded in a subring Λ of P on which $\mathfrak{G}$ induces a finite regular automorphism group $\mathfrak{G}_\Lambda$ over Φ. Each element of $\mathfrak{M}(\Sigma)$ can be then extended to an element of $\mathfrak{M}(\Lambda)$, in other words, $\mathfrak{M}(\Sigma)$ is considered to be the restriction of $\mathfrak{M}(\Lambda)$ to Σ. But $\mathfrak{M}(\Lambda)=\mathfrak{G}_\Lambda \mathrm{P}_r$ since the elements of P_r-basis of $\mathfrak{M}(\Lambda)$ in the sens of Lemma 2 are contained already in $\mathfrak{G}_\Lambda \Lambda_r$. Hence $\mathfrak{M}(\Sigma)=\mathfrak{G}_\Sigma \mathrm{P}_r$.

Theorem 3. (EXTENSION THEOREM) *Let the maximal automorphism group* $\mathfrak{G}$ *of* P/Φ *be locally finite For any subring* Σ *of* P *containing* Φ, *any isomorphism* T' *of* Σ *into* P *which is the identity on* Φ *can be extended to an automorphism* T *of* P.

Proof. 1°. First assume that $[\Sigma:\Phi]_l<\infty$. Then $T'\in\mathfrak{M}(\Sigma)=\mathfrak{G}_\Sigma \mathrm{P}_r$ by Lemma 4. Since $T'\mathrm{P}_r$ is an irreducible $\Sigma_r-\mathrm{P}_r$ two-sided module, it is isomorphic to $S_\Sigma \mathrm{P}_r$ for some element S of $\mathfrak{G}$. As in the proof of Theorem 2, we can show that $T'=S_\Sigma I=(SI)_\Sigma$ for some inner automorphism I of $\mathfrak{G}$. If we put $SI=T$, T is an extension of T'.

2°. Generally let Σ be the join of the subrings Σ_α which are finite over $\Phi:\Sigma=\bigvee_\alpha \Sigma_\alpha$. Let T_α' be the restriction of T' to Σ_α. T_α' is always extendable to an automorphism of P by 1°; we denote the set of all these extensions of T_α' by E_α. Then E_α is a topologically closed set. If $\bigwedge_\alpha E_\alpha=\phi$, then there exist a finite number of α_i $(i=1,\cdots,m)$ such that $\bigwedge_{i=1}^m E_{\alpha i}=\phi$, for $\mathfrak{G}$ is a compact group. If we consider Σ_β which is generated by Σ_{α_i} $(i=1,\cdots,m)$, then $E_\beta=\bigwedge_{\alpha_i} E_{\alpha_i}=\phi$. This is a contradiction by 1°. Now any element T of $\bigwedge_\alpha E_\alpha$ is the required extension of T'.

If $\mathfrak{G}$ is a locally finite automorphism group, then P is locally finite over Φ and it is possible to introduce a Haussdorf topology in $\mathfrak{G}$.[6] In [7] the present author showed the fundamental correspondence between topologically closed regular subgroups and subrings when the maximal automorphism group $\mathfrak{G}$ of P/Φ is locally finite. But it will be shown that, if $\mathfrak{G}$ is a locally finite regular automorphism group of P/Φ, its topological closure $\bar{\mathfrak{G}}$ is the maximal automorphism group of P/Φ which is naturally locally finite.

Theorem 4. *If* $\mathfrak{G}$ *is a locally finite regular automorphism group of* P/Φ, *then its topological closure* $\bar{\mathfrak{G}}$ *is the maximal automorphism group of* P/Φ.

6) See [7].

Proof. Let T be any automorphism of P leaving each element of Φ invariant and Σ any subring containing Φ which has a finite rank over Φ. Then $T_\Sigma \in \mathfrak{M}(\Sigma) = \mathfrak{G}_\Sigma P_r$ by Lemma 4 and, as in the proof of Theorem 2, $T_\Sigma = (SI)_\Sigma$ where $SI \in \mathfrak{G}$ since $\mathfrak{G}$ is regular. This implies $T \in \bar{\mathfrak{G}}$.

Let Σ be a subring of P containing Φ, and $\mathfrak{H}$ the subgroup of $\mathfrak{G}$ consisting of all the automorphisms of $\mathfrak{G}$ which leave Σ setwise invariant.

Theorem 5. (NORMALITY THEOREM) *Let the maximal automorphism group* $\mathfrak{G}$ *of* P$/\Phi$ *be locally finite. Then* Σ *is a Galois extension of* Φ *(that is, there exists an automorphism group of* Σ/Φ*) if and only if the topological closure* $\bar{\mathfrak{H}}^*$ *of the regularization* $\mathfrak{H}^*$ *of* $\mathfrak{H}$ *is equal to* $\mathfrak{G}$.

Proof. First assume that Σ is a Galois extension of Φ. Since any automorphism of Σ which is the identity of Φ is extendable to an automorphism of P, that is, to an automorphism contained in $\mathfrak{H}$, and since $\Phi(\mathfrak{G}(\Sigma)) = \Sigma$,[7] Φ is the same as the ring of all the $\mathfrak{H}$-invariant elements of P. This implies that $\mathfrak{H}^*$ is a regular automorphism group of P/Φ. Then $\bar{\mathfrak{H}}^* = \mathfrak{G}$ by Theorem 4.

Next assume that $\bar{\mathfrak{H}}^* = \mathfrak{G}$. Let Ψ be the ring of all the $\mathfrak{H}$-invariant elements. Then, as before, $\bar{\mathfrak{H}}^*$ is the maximal automorphism group of P$/\Psi$ and hence $\Psi = \Phi$. Of course $\mathfrak{H}$ is an automorphism group of Σ/Φ, this is, Σ is a Galois extension of Φ.

§ 3. Structure of the Galois extensions.

Using a result due to Kasch, it will be proved that, if P is a Galois extension of Φ with the locally finite maximal automorphism group $\mathfrak{G}$, then any subring which is finite over Φ is simply generated over Φ. We always assume that Φ is not a finite field, for, if Φ is a finite field, P becomes a field and the assertion is clear.

Lemma 5. (KASCH) *Let* Σ *be a subring of* P *containing* Φ. *For any finite number of element* $s_1, s_2, \cdots, s_n$ *of* $\mathfrak{M}(\Sigma)$, *non of which is the identity mapping, there exists an element* σ *of* Σ *such that* $\sigma s_i \neq \sigma$ $(i = 1, \cdots, n)$.

Proof. We shall prove the lemma by induction. Since it is clear when $n=1$, assume that the lemma is true for $s_1, s_2, \cdots, s_{n-1}$. Then there exists an element σ' of Σ such that $\sigma' s_i \neq \sigma'$ $(i=1, \cdots, n-1)$. On

7) $\mathfrak{G}(\Sigma)$ implies the subgroup of $\mathfrak{G}$ consisting of all the automorphisms in $\mathfrak{G}$ which leave each element of Σ invariant, and $\Phi(\mathfrak{H})$ implies the subring of all the $\mathfrak{H}$-invariant elements.

the other hand let σ'' be such an element of Σ that $\sigma'' s_n \neq \sigma''$. Now we consider the element $\sigma' + \varphi\sigma''$ where φ is any element of Φ. We have $(\sigma' + \varphi\sigma'')s_i - (\sigma' + \varphi\sigma'') = (\sigma' s_i - \sigma') + \varphi(\sigma'' s_i - \sigma'')$. Since $\sigma' s_i - \sigma' \neq 0$ for $i = 1, \cdots, n-1$, and $\sigma'' s_i - \sigma'' \neq 0$ for $i = n$, there exist only a finite number of elements φ in Φ such that they satisfy the equality: $(\sigma' s_i - \sigma') + \varphi(\sigma'' s_i - \sigma'') = 0$ for some i. But Φ is assumed to contain infinitely many elements and hence there exists such an elemeot θ in Φ that, if we put $\sigma = \sigma' + \theta\sigma''$, then $\sigma s_i \neq \sigma$ for $i = 1, \cdots, n$, which completes the proof of Lemma 5.

Theorem 6. *If* P *is a Galois extension of* Φ *with a locally finite regular automorphism group* $\mathfrak{G}$, *and if* Σ *is a subring containing* Φ *which has a finite rank over* Φ, *then there exists an element* α *in* Σ *such that* Σ *is generated by* α *and* Φ.

Proof. We have $\mathfrak{M}(\Sigma) = \mathfrak{G}_\Sigma \mathrm{P}_r$ by Lemma 4 and we apply Lemma 5 to all the elements of $\mathfrak{G}_\Sigma$ except the identity mapping ($\mathfrak{G}_\Sigma$ is a finite set.). Then we can find an element α in Σ such that α is really moved by any element of $\mathfrak{G}_\Sigma$ except the identity mapping. It will be shown that Σ is then generated by α and Φ. For, if it is not so, there exists an element of β such that $\beta S \neq \beta$ and $\alpha S = \alpha$ by Galois theory, which is a contradiction since α is moved by S_Σ.

Corollary. *Under the same conditions as in Theorem* 6, *there exists an element* α *in* Σ *such that* α *is mapped to all its different images by the elements of* $\mathfrak{G}_\Sigma$.

Proof. We may choose an element α such that Σ is generated by α and Φ. Then each element of $\mathfrak{G}_\Sigma$ is uniquely determined by its restriction to α.

Remark. In the case that $\mathfrak{G}$ is an outer group, if $[\Sigma : \Phi]_l = n$, then the number of different images of α is n.

(Received March 28, 1956)

References

[1] H. Cartan: Théorie de Galois pour les corps non commutatifs, Ann. Sci. Ecole Norm. Sup. **64** (1947).

[2] N. Jacobson: The fundamental theorem of Galois theory for quasifields, Ann. of Math. **41** (1940).

[3] N. Jacobson: A note on division rings, Amer. J. Math. **69** (1947).
[4] F. Kasch: Über den Satz vom primitiven Element bei Schiefkörpern, J. Reine Angew. Math. **189** (1951).
[5] T. Nagahara and H. Tominaga: A note on Galois theory of division rings of infinite degree, Proc. Japan Acad. **31** (1955).
[6] T. Nakayama: Galois theory of simple rings, Trans. Amer. Math. Soc. **73** (1952).
[7] N. Nobusawa: An extension of Krull's Galois theory to division rings, Osaka Math. J. **7** (1955).