Osaka Mathematical Journal
Vol. 7, No. 1, June, 1955.

An Extension of Krull's Galois Theory to Division Rings

By Nobuo NOBUSAWA

Galois theory was extended to division rings by N. Jacobson and H. Cartan, and to more general rings by G. Azumaya and T. Nakayama. In this paper we shall extend it in the case of infinite degree.

Let $\mathfrak{G}$ be a group of automorphisms of a division ring P, and let Φ be the subring of all the $\mathfrak{G}$-invariant elements of P. If $\mathfrak{G}$ contains all the inner automorphisms of P which leave each element of Φ invariant, we call $\mathfrak{G}$ *regular*.

In § 1, we shall show that, if $\mathfrak{G}$ is regular and $[P:\Phi]_l < \infty$, there exists Galois correspondence between regular subgroups of $\mathfrak{G}$ and subrings of P containg Φ. But if $[P:\Phi]_l < \infty$, the regular group is Jacobson's closed group of finite reduced order and conversely.

In § 2, we consider the case of infinite degree. We assume that P is locally finite over Φ, that is, any subring generated by Φ and a finite number of elements of P has finite (left) rank over Φ. Let $\mathfrak{G}$ be the maximal group of automorphisms of P leaving each element of Φ invariant. Further we assume that each element of P is mapped at most to a finite number of elements of P by $\mathfrak{G}$. Then we can introduce a topology in $\mathfrak{G}$ and show that there exists Galois correspondence between (topologically) closed regular subgroups of $\mathfrak{G}$ and subrings of P containing Φ.

§ 1. Galois theory of finite degree.

First we quote two theorems from Jacobson's paper [4] with respect to commuter systems of endomorphism rings of the module P. Let P be a division ring and let $\mathfrak{A}$ be the absolute endomorphism ring of the module P. P_r shows the subring of $\mathfrak{A}$ generated by right multiplications of the elements of P. Similarly we define P_l and Φ_l for a subring Φ of P.

Let $\mathfrak{B}$ be a subring of $\mathfrak{A}$ that contains P_r. Then its commuter system $V(\mathfrak{B})$ in $\mathfrak{A}$ is a subring of $V(P_r) = P_l$, and has a form $V(\mathfrak{B}) = \Phi_l$ with a subring Φ of P.

Theorem 1. *If* $[\mathfrak{B}: \mathrm{P}_r]_r = n < \infty$ *and* $V(\mathfrak{B}) = \Phi_l$, *then* $V(V(\mathfrak{B})) = \mathfrak{B}$ *and* $[\mathrm{P}: \Phi]_l = n$.

Theorem 2. *If* Φ *is a subring of* P *and* $[\mathrm{P}: \Phi]_l = n < \infty$, *then* $V(V(\Phi_l)) = \Phi_l$ *and* $[V(\Phi_l): \mathrm{P}_r]_r = n$.

Let P be a division ring and Φ its subring, Then we mean by a group of P/Φ an automorphism group $\mathfrak{G}$ of P which has Φ as the subring of all the $\mathfrak{G}$-invariant elements of P.

DEFINITION. If a group of P/Φ contains all the inner automorphisms which leave each element of Φ invariant, we call it a regular group of P/Φ.

Let $\mathfrak{G}$ be a group of P/Φ, and S one of its elements. Then $S\mathrm{P}_r$ is a P_r-two sided irreducible module. Let also $\mathfrak{M}$ be a subring of $\mathfrak{G}\mathrm{P}_r$ containing P_r, then $\mathfrak{M}$ is also a P_r-two sided module.

Lemma 1. *If* $\mathfrak{M} \cong S\mathrm{P}_r$ *and an element* s *of* $\mathfrak{M}$ *corresponds to* S, *then* $s = S(1 \cdot s)_l$.

Proof. For any α in P, $\alpha_r s$ corresponds to $\alpha_r S = S(\alpha \cdot S)_r$, hence $\alpha_r \cdot s = s(\alpha \cdot S)_r$. Therefore $\alpha \cdot s = 1 \cdot \alpha_r s = 1 \cdot s(\alpha \cdot S)_r = \alpha \cdot S(1 \cdot s)_l$.

Theorem 3. *Let* $\mathfrak{G}$ *be a group of* P/Φ. *If* $[\mathrm{P}: \Phi]_l < \infty$, *then any automorphism* T *of* P *which leaves each element of* Φ *invariant can be written in the form*: $T = SI$, *with some element* S *of* $\mathfrak{G}$ *and an inner automorphism* I *of* P.

Proof. As $V(\mathfrak{G}\mathrm{P}_r) = \Phi_l$, it is seen by Theorems 1 and 2 that $V(\Phi_l) = \mathfrak{G}\mathrm{P}_r$. Then T is contained in $V(\Phi_l) = \mathfrak{G}\mathrm{P}_r$, and hence $T\mathrm{P}_r$ is isomorphic to a P_r-two sided irreducible module $S\mathrm{P}_r$ with some element S of $\mathfrak{G}$: $T\mathrm{P}_r \cong S\mathrm{P}_r$. If $T\rho_r (\rho \in \mathrm{P})$ corresponds to S, then by Lemma 1 $T\rho_r = S(1 \cdot T\rho_r)_l = S\rho_l$. Then $T = S\rho_l\rho_r^{-1} = SI$.

REMARK. If $\mathfrak{G}$ contains no inner automorphism, $\mathfrak{G}\mathrm{P}_r$ is the direct sum of P_r-two sided irreducible submodules which are not isomorphic to each other, and hence $T\mathrm{P}_r = S\mathrm{P}_r$, that is, $T = S$.

This theorem shows a regular group of P/Φ is the maximal group of P/Φ if $[\mathrm{P}: \Phi]_l < \infty$.

Lemma 2. *Let* $\mathfrak{G}$ *be the regular group of* P/Φ, *and* $\mathfrak{M}$ *a subring of* $\mathfrak{G}\mathrm{P}_r$ *containing* P_r. *Then* $\mathfrak{M} = (\mathfrak{G} \cap \mathfrak{M})\mathrm{P}_r$.

Proof. Assume $\mathfrak{M} \neq (\mathfrak{G} \cap \mathfrak{M})\mathrm{P}_r$, then $\mathfrak{M} - (\mathfrak{G} \cap \mathfrak{M})\mathrm{P}_r$ contains a P_r-two sided irreducible submodule $\mathfrak{N}$ and $\mathfrak{N} \cong S\mathrm{P}_r$ with some element

S of $\mathfrak{G}$. If s in $\mathfrak{N}$ corresponds to S, then $\mathfrak{N}=s\mathrm{P}_r=S(1\cdot s)_l\mathrm{P}_r=SI\mathrm{P}_r$ with some inner automorphism I by Lemma 1. But as $\mathfrak{G}$ is regular $SI\in\mathfrak{G}$ and also $SI\in\mathfrak{N}\leqq\mathfrak{M}$, that is, $\mathfrak{N}=SI\mathrm{P}_r\leqq(\mathfrak{M}\cap\mathfrak{G})\mathrm{P}_r$, which contradicts the assumption.

Theorem 4. *If* $[\mathrm{P}:\Phi]_l<\infty$ *and* $\mathfrak{G}$ *is the regular group of* P/Φ, *then between regular subgroups* $\mathfrak{H}$ (*that is,* $\mathfrak{H}$ *is the regular group of* $\mathrm{P}/\sum$: $\sum$ *is the subring of all the* $\mathfrak{H}$*-invariant elements.*) *and subrings* $\mathfrak{M}$ *of* $\mathfrak{G}\mathrm{P}_r$ *containing* P_r *there exists a one-to-one correspondence with the following relations*: $\mathfrak{H}=\mathfrak{M}\cap\mathfrak{G}$ *and* $\mathfrak{M}=\mathfrak{H}\mathrm{P}_r$.

Proof. For a given $\mathfrak{M}$, let $\mathfrak{H}$ be the intersection of $\mathfrak{M}$ aud $\mathfrak{G}$, then $\mathfrak{H}$ is a group because $\mathfrak{H}$ has no zero divisor and any non zero divisor in $\mathfrak{M}$ has its inverse since $\mathfrak{M}$ is finite over P_r. $\mathfrak{H}$ is regular because $\mathfrak{G}$ is regular and $V(V(\mathfrak{M}))=\mathfrak{M}$. Then by Lemma 2 $\mathfrak{M}=\mathfrak{H}\mathrm{P}_r$.

Conversely for a given regular group $\mathfrak{H}$, let $\mathfrak{M}=\mathfrak{H}\mathrm{P}_r$, then $\mathfrak{H}=\mathfrak{M}\cap\mathfrak{G}$ as $\mathfrak{H}$ is regular (whence maximal) and $V(\mathfrak{M})=V(\mathfrak{H})$.

Theorems 1,2 and 4 establish Galois theory in the case of finite degree.

Next we show that our regular group is Jacobson's closed group.

Lemma 3. *Let* $\tau_1,\tau_2,\cdots,\tau_h$ *be the elements of* P. *If* $\tau_{1l},\tau_{2l},\cdots,\tau_{hl}$ *are linearly inpependent over* P_r, *then* $\tau_1,\tau_2,\cdots,\tau_h$ *are linearly independent over the center* Γ *of* P *and conversely.*

Proof. As $\gamma_l=\gamma_r$ for any element γ in Γ, the first part is clear. We assume $\tau_{1l},\tau_{2l},\cdots,\tau_{hl}$ are linearly dependent over P and

$$\tau_{1l}\mu_{1r}+\tau_{2l}\mu_{2r}+\cdots+\tau_{sl}\mu_{sr}=0\qquad(0<s\leqq h)$$

is the shortest non-trivial relation. We may put $\mu_1=1$. We can show all the μ_i $(i=1,2,\cdots,s)$ are in Γ. For this, assume $\mu_s\notin\Gamma$, then there exists an element ν of P such that $\nu\mu_s-\mu_s\nu\neq0$. Then the relation

$$\nu_r(\tau_{1l}\mu_{1r}+\tau_{2l}\mu_{2r}+\cdots+\tau_{sl}\mu_{sr})-(\tau_{1l}\mu_{1r}+\tau_{2l}\mu_{2r}+\cdots+\tau_{sl}\mu_{sr})\nu_r=0$$

is shorter than before. This proves the converse part of the Lemma.

Theorem 5. *Assume* $[\mathrm{P}:\Phi]_l=n<\infty$, *and let* $\mathfrak{G}$ *be the regular group of* P/Φ *and* $\mathfrak{H}$ *the subgroup of all the inner automorphisms contained in* $\mathfrak{G}$. *Then* $\mathfrak{H}$ *has a finite index* u *in* $\mathfrak{G}$ *and the set of all the elements which define the elements of* $\mathfrak{H}$ *is the division algebra with finite rank* h *over the center* Γ *of* P. *Then* $n=uh$.

Proof. As $[\mathfrak{G}\mathrm{P}_r:\mathrm{P}_r]_r=[\mathrm{P}:\Phi]_l=n$, $\mathfrak{G}\mathrm{P}_r$ must be the direct sum

of n P_r–two sided irreducible modules:

$$\mathfrak{G}P_r = S_1P_r + S_2P_r + \cdots + S_nP_r \quad (S_i \in G).$$

It is easily seen that, if $S_iP_r \cong S_jP_r$, then $S_i = S_jI$ with some inner automorphism $I = I_{i,j}$ and conversely. Then using Lemma 3, we can prove the theorem.

The converse of this theorem is also true. It was given by Jacobson in [4].

§ 2. Galois theory of infinite degree.

We do not assume that $[P:\Phi]_l < \infty$ in this chapter, but assume always that P/Φ is locally finite, by which we mean that any ring $(\Phi, \rho_1, \rho_2, \cdots \rho_m)$ generated by Φ and a finite number of elements ρ_i of P has finite left rank over Φ. Throughout this chapter we assume also $\mathfrak{G}$ is the maximal group of P/Φ.

DEFINITION. A subring Σ of P containing Φ is said to be *normal* when $\mathfrak{G}$ induces a group $\mathfrak{G}_\Sigma$ of Σ/Φ.

DEFINITION. A subring Σ of P containing Φ is said to be *finite over* Φ if $[\Sigma:\Phi]_l < \infty$.

Lemma 4. *If Σ is normal and finite over Φ, then $\mathfrak{G}$ induces the maximal group $\mathfrak{G}_\Sigma$ of Σ/Φ.*

Proof. $\mathfrak{G}_\Sigma$ is of course a group of Σ/Φ, but $\mathfrak{G}_\Sigma$ must be regular since any inner automorphisms of Σ can be extended to inner automorpeisms of P. Then $\mathfrak{G}_\Sigma$ is maximal since Σ is finite over Φ.

REMARK. Later we shall prove that this lemma holds without finiteness assumption on Σ.

We can introduce a topology in $\mathfrak{G}$ as Krull [8] did under the following assumption under which P/Φ is of course locally finite.

ASSUMPTION. *Each element of* P *is mapped by $\mathfrak{G}$ at most to a finite number of elements of* P.

This assumption is satisfied if each polynomial over Φ has at most a finite number of roots in P, and of course in the case of commutative fields it is satisfied. In the case of finite degree an outer automorphism group satisfies it since the group is of finite order.

Under this assumption we define neighbourhoods $U(S;\Sigma)$ of elements S of $\mathfrak{G}$ with normal subrings Σ which are finite over Φ such as $U(S;\Sigma)=\{T\in\mathfrak{G};\ \alpha S=\alpha T \text{ for any } \alpha \text{ in } \Sigma\}$.

The neighbourhoods satisfy the following Haussdorff's axioms;

(1) $S\in U(S;\Sigma)$.

(2) $U(S;\Sigma)\cap U(S;\Sigma')=U(S;\Sigma\cup\Sigma')$.

(3) If $T\in U(S;\Sigma)$, then $U(S;\Sigma)=U(T;\Sigma)$.

(4) If $S\neq T$, then there exist $U(S;\Sigma)$ and $U(T;\Sigma')$ such that $U(S;\Sigma)\cap U(T;\Sigma')=\phi$.

For (2), see that $\Sigma\cup\Sigma'$ is finite over Φ since P/Φ is locally finite. For (4), choose α in P such that $\alpha S\neq\alpha T$ and consider the least normal extension of (Φ,α) which is finite over Φ by our assumption.

Our assumption implies that for any subring which is finite over Φ its least normal extension is also finite over Φ, and for a finite normal subring Σ the induced group $\mathfrak{G}_\Sigma$ is of finite order. Then $\mathfrak{G}$ is a compact group because $\mathfrak{G}$ is the projective limit of finite (and hence compact) groups $\mathfrak{G}_{\Sigma_\alpha}$ which are groups of Σ_α/Φ: Σ_α are all the finite normal subrings of P. The theorem of limit groups implies that $\mathfrak{G}$ is compact.

For a subring Σ of P containing Φ, we mean by $\mathfrak{G}(\Sigma)$ the group of all the automorphisms of P which leave each element of Σ invariant. Similarly for a subgroup $\mathfrak{H}$ of $\mathfrak{G}$ we mean by $\Phi(\mathfrak{H})$ the subring of P of all the elements left invariant by $\mathfrak{H}$.

Lemma 5. *If* $[\Sigma:\Phi]_l<\infty$, *then* $\Phi(\mathfrak{G}(\Sigma))=\Sigma$.

Proof. If $\Phi(\mathfrak{G}(\Sigma))\neq\Sigma$, there exists such a ρ as contained in $\Phi(\mathfrak{G}(\Sigma))$ but not contained in Σ. Let Σ' be the least normal extension of (Σ,ρ), then Σ' is of course finite over Φ and $\mathfrak{G}_{\Sigma'}$ is the regular group of Σ'/Φ, and hence there exists an element S in $\mathfrak{G}_{\Sigma'}$ such that it moves ρ but not each element of Σ, which contradicts the assumption on ρ.

Theorem 6. $\Phi(\mathfrak{G}(\Sigma))=\Sigma$ *for any subring* Σ *of* P *containing* Φ, *and* $\mathfrak{G}(\Phi(\mathfrak{H}))=\mathfrak{H}$ *if* $\mathfrak{H}$ *is the maximal group of* $P/\Phi(\mathfrak{H})$.

Proof. Assume ρ to be in $\Phi(\mathfrak{G}(\Sigma))$ but not in Σ. Let $\Sigma=\bigcup_\alpha\Sigma_\alpha$ with subrings Σ_α which are finite over Φ, then $\mathfrak{G}(\Sigma)=\bigcap_\alpha\mathfrak{G}(\Sigma_\alpha)$. Let M_α be the subset of $\mathfrak{G}(\Sigma_\alpha)$ of all the elements which move ρ, then $\bigcap_\alpha M_\alpha=\phi$ as $\mathfrak{G}(\Sigma)$ contains no element which moves ρ. But $\mathfrak{G}$ is compact and each M_α is closed, so there exist a finite number of M_{α_i} $(i=1,2,\cdots,n)$ such that $\bigcap_i M_{\alpha_i}=\phi$. But $\Sigma'=\bigcup_i\Sigma_{\alpha_i}$ is finite over Φ and hence by Lemma 5 there exists an automorphism which moves ρ and not each element of Σ', which contradicts the fact $\bigcap_i M_{\alpha_i}=\phi$.

By this theorem we have the one-to-one correspondence between maximal subgroups of $\mathfrak{G}$ and subrings of P containing Φ.

Theorem 7. *A (topologically) closed regular group is a maximal group and conversely.*

Proof. Let $\mathfrak{H}$ be a (topologically) closed regular group of $P/\Phi(\mathfrak{H})$, and T any automorphism of P leaving each element of $\Phi(\mathfrak{H})$ invariant. We shall show T is in $\mathfrak{H}$. Let Σ be any normal extension which is finite over Φ, then $\mathfrak{H}$ induces the maximal group of $\Sigma\bigcup\Phi(\mathfrak{H})/\Phi(\mathfrak{H})$ since $\mathfrak{H}$ is regular and $\Sigma\bigcup\Phi(\mathfrak{H})$ is finite over $\Phi(\mathfrak{H})$. But T also induces an automorphism of $\Sigma\bigcup\Phi(\mathfrak{H})$ leaving each element of $\Phi(\mathfrak{H})$ invariant, and hence there exists an element S in $\mathfrak{H}$ such that $\alpha S=\alpha T$ for any elements α in Σ. In other words, $T\in U(S;\Sigma)$. But $\mathfrak{H}$ is closed and hence T is in $\mathfrak{H}$.

Conversely if $\mathfrak{H}$ is a maximal group, it is of course regular. If T is a limit point of $\mathfrak{H}$, then for any α in $\Phi(\mathfrak{H})$ we can show $\alpha T=\alpha$. For, $\alpha T=\alpha S$ with some element S of $\mathfrak{H}$ since $T\in U(S;\Sigma)$ with any finite normal subring $\sum$ containing α, but $\alpha S=\alpha$. Hence $T\in\mathfrak{H}$, that is, $\mathfrak{H}$ is (topologically) closed.

Thus we have the one-to-one correspondence between (topologically) closed regular subgroups of $\mathfrak{G}$ and subrings of P containing Φ. If $\mathfrak{G}$ does not contain any inner automorphism except the unity automorphism, all the closed subgroups are necessarily maximal.

For any normal subring Σ, $\mathfrak{G}_\Sigma$ is closed and regular so the remark to Lemma 4 is clear.

By the way we can extend this theory to simple rings by Nakayama's method.

(Received March 10, 1955)

References

[1] G. Azumaya, Galois theory for uni-serial rings, J. Math. Soc. Jap. **1** (1949).
[2] H. Cartan, Théorie de Galois pour les corps non commutatifs, Ann. Ecole Norm. Sup. **64** (1947).
[3] N. Jacobson, The fundamental theorem of Galois theory for quasifields, Ann. Math. **41** (1940).
[4] N. Jacobson, A note on division rings, Amer. J. Math. **69** (1947).
[5] T. Nakayama, Galois theory for general rings with minimum condition, J. Math. Soc. Japan. **1** (1949).
[6] T. Nakayama, Galois theory of simple rings, Trans. Amer. Math. Soc. **73** (1952).
[7] T. Nakayama and G. Azumaya, On irreducible rings, Ann. Math. **48** (1947).
[8] W. Krull, Galoische Theorie der unendlichen algebraischer Erweiterungen, Math. Ann. **100** (1928).