ON GALOIS CONDITIONS IN DIVISION ALGEBRAS

By Motoichi Okuzumi

1. Introduction.

A division subring A of a division ring D is said to be Galois in D (and D is Galois over A), if A is the set of fixed elements of a group of automorphisms acting in D. When that is so, as commutative case, there is one to one correspondence between a division subring B of D over A and a closed group H of automorphisms of D with finite reduced order. And, in commutative case, we know that the necessary and sufficient conditions for D to be Galois over A are: D is finite, separable and normal over A. Jacobson, developing Galois theory in division rings, had shown that it is an unsolved problem to determine conditions on a division subring A of D in order that there exists a closed group G of finite reduced order whose ring of the fixed elements is A. And he had proved the following result which is in essence due to Teichmüller:

If Z_0 is a subfield of the center Z of a division ring D and $[D:Z]$ is finite, then necessary and sufficient conditions that there exists a closed group G of automorphisms whose set of fixed elements is Z_0 are

1) Z is separable and normal over Z_0 and
2) every automorphism of the Galois group of Z over Z_0 can be extended to an automorphism of D.

In the present paper we shall derive conditions for D to be Galois over its division subring A in the case of finite dimension over the center. In the followings we assume that the center of D has an infinite number of elements.

2. Central elements in a division ring.

In the followings we denote by $V_S(A)$ the set of all elements of S which are commutative with every element of A. Then,

Lemma 1. *If R is a ring with unit element e and center Z, and A is a subring of R containing e, then*

$$V_R(A)=V_R(A,Z),$$

where (A,Z) is the ring generated by A and Z.

Proof. It is evident that $V_R(A,Z)$ is contained in $V_R(A)$. If c is any element of $V_R(A)$ and a is any element of (A,Z), then

Received July 5, 1965.

$$a=\sum_{i=1}^{n} a_i z_i,\ a_i \in A,\ z_i \in Z \qquad ac=\sum_{i=1}^{n} a_i c z_i=\sum_{i=1}^{n} c a_i z_i=ca.$$

DEFINITION. Let R be a ring with unit element e and center Z. A subring A of R is said to be *regular* if $V_R(V_R(A))=(A, Z)$ and contains the unit element of R.

In our case of division rings, any division subring is regular.

LEMMA 2. *Let R be a ring with unit element e and center Z. If A and B are regular subrings such that $A \supset B$ and $V_R(A)=V_R(B)$, then $A \subset (B, Z)$.*

Proof. $V_R(A)=V_R(A, Z)=V_R(B, Z)=V_R(B)$.
From regularity of A and B, $(A, Z)=(B, Z)$ and $A \subset (B, Z)$.

When subrings A and B are as in lemma 2, we say that A is a central extension of B, that is, A is generated by adjunction of central elements of R. When a division ring D is Galois over its division subring A, then the commutator algebra N of $V_R(A)$ is a central extension of A.

Next, we shall derive a property of central elements in a division ring.

LEMMA 3. *Let D be a division ring with center Z, let Z_0 be a subfield of Z such that Z is a Galois extension field of Z_0, and let α be a generating element of Z over Z_0. If β is an element of D such that $Z_0(\beta)$ is isomorphic with $Z_0(\alpha)$ leaving the elements of Z_0 invariant, then β is contained in the center of D.*

Proof. Let K be the field generated by β over Z_0: $K=Z_0(\beta)$. We adjoin α to K, then $K(\alpha)$ is a finite extension field of Z_0. But, in a commutative field, an isomorphic element is a conjugate element, so β is contained in Z.

COROLLARY 1. *Under the same assumptions in lemma 3, let Δ be a subfield of Z over Z_0 and Δ' a subfield of D isomorphic with Δ over Z_0, then Δ' is contained in Z.*

The proof is similar to that of lemma 3.

In the case of a simple ring, this lemma is not valid in general. For example, let D be a total matrix ring $[Z]_n$, and let the defining equation of α which is a generating element of Z over Z_0

$$f(x)=x^n+a_1x^{n-1}+\cdots+a_{n-1}x+a_n=0.$$

Then the matrix

$$\beta=\begin{bmatrix} 0 & 1 & 0 & \cdots & \cdots & 0 \\ 0 & 0 & 1 & 0 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ -a_1 & -a_2 & \cdots & \cdots & \cdots & -a_n \end{bmatrix}$$

has $f(x)=0$ as its defining equation. Therefore, $Z_0(\beta)$ is isomorphic with $Z_0(\alpha)$, but β is not contained in the center.

LEMMA 4. *Let D be a division ring with center Z, let Z_0 be a subfield of Z such that Z is Galois over Z_0, and let $f(x)=0$ be the defining equation of α which is a generating element of Z over Z_0. If A is a division subring of D such that $A\frown Z=Z_0$, then the polynomial $f(x)$ is irreducible in $A[x]$.*

Proof. $A[x]$ is a semi-commutative polynomial ring in Kasch's meaning, and is a principal ideal ring. If $f(x)$ is reducible in $A[x]$ and let $h(x)$ be the minimum polynomial of α in $A[x]$, then $h(x)$ is a divisor of $f(x)$. But, by lemma 3, all roots of $h(x)$ lie in Z and $h(x)$ is a polynomial in $Z_0[x]$. So, $f(x)$ has $h(x)$ as a divisor in $Z_0[x]$. This is a contradiction.

THEOREM 1. *Let D be a division ring with center Z, and let A be a division subring of D such that $A\frown Z=Z_0$, $[A:Z_0]$ is finite and Z is Galois over Z_0, then any isomorphism of A into D leaving the elements of Z_0 invariant can be extended to an inner automorphism of D.*

Proof. Let B be the isomorphic image of A in D, then by corollary 1, $B\frown Z=Z_0$. So, by lemma 4, the composite division subring $A(\alpha)$ and $B(\alpha)$ becomes isomorphic to each other leaving the elements of Z invariant, where α is a generating element of Z over Z_0. Therefore, by the well known theorem, the isomorphism can be extended to an inner automorphism of D.

Under the same assumptions in theorem 1, we obtain the following theorem.

THEOREM 2. *D is Galois over A, if and only if D is Galois over $A\frown Z=Z_0$.*

Proof. Let D be Galois over A, G the Galois group of D/A and H the subgroup of inner automorphisms in G. The automorphisms σ of G induce automorphisms $\bar{\sigma}$ in the center Z and the induced groug $\bar{G}$ of G in Z is isomorphic with G/H. Then, the fixed field of $\bar{G}$ is $A\frown Z=Z_0$ and Z is Galois over Z_0. Therefore, Jacobson-Teichmüller's conditions are satisfied and D becomes Galois over Z_0.

Conversely, if D is Galois over $A\frown Z$, then every automorphism σ maps A onto A^σ and by theorem 1, this isomorphism can be extended to an inner automorphism τ. But the Galois group of D/Z_0 contains every inner automorphism. So, $\sigma\tau^{-1}$ are automorphisms of D leaving the elements of A invariant. Therefore, we can select a set of automorphisms of D/Z which induce distinct automorphisms of Z/Z_0 and leaving the elements of A invariant. If we adjoin to them all inner automorphisms induced by elements of $V_D(A)$, then we obtain a closed group G of automorphisms of D. Let σ be an automorphism leaving A invariant, then σ must be contained in G. And let A_1 be the fixed ring for G, then A_1 must be central extension of A and A_1 corresponds to the automorphism group of Z/Z_0. So, $A_1=A$. Therefore, D is Galois over A.

3. Generating elements in a division ring.

Let D be a non-commutative division ring with center Z, and let A be a proper division subring not contained in Z and $[Z:Z\frown A]=n$. Let $D^{\times}$ denote the multiplicative group of all non-zero elements of D, then $[D^{\times}:A^{\times}]$ is infinite. This is proved by Faith. Similarly, the additive group A^{+} has infinite index in D^{+}. For, suppose A^{+} has finite index in D^{+}. Then for any element d in D, there are elements c_1, c_2 and a such that

$$dc_1=dc_2+a, \qquad c_1, c_2 \in Z\frown A, \qquad a \in A.$$

But, $c_1 \neq c_2$, so this contradicts $A \neq D$.

First, we introduce the concept of union-coset in groups. Let G be a group of infinite order, and $H_1, H_2, \cdots, H_n$ its subgroups of infinite indices. If $a_1H_1, a_2H_2, \cdots, a_nH_n$ are right cosets of $H_1, H_2, \cdots, H_n$ in G, then the union of these cosets $a_1H_1 \smile a_2H_2 \smile \cdots \smile a_nH_n$ is called a union coset of degree n.

Under these assumptions, we prove the following lemma and then show a simple proof of Albert-Kasch-Nagahara's generating theorem in division rings.

LEMMA 5. *G can not be covered by a finite number of union-cosets, of any finite degree.*

Proof. For $n=1$, the assertion is obvious, therefore, assume it to be correct for $n-1$. Suppose G is covered by a finite number of union-cosets as follows:

$$G=a_1H_1 \smile a_2H_2 \smile \cdots \smile a_nH_n + b_1H_1 \smile b_2H_2 \smile \cdots \smile b_nH_n + \cdots + d_1H_1 \smile d_2H_2 \smile d_nH_n.$$

But, G can not be covered by union-cosets of degree $n-1$ from the assumption of induction, so there is an infinite covering of G containing

$$a_1H_1 \smile a_2H_2 \cdots \smile a_{n-1}H_{n-1} + \cdots + d_1H_1 \smile d_2H_2 \smile \cdots \smile d_{n-1}H_{n-1}.$$

Let the covering be as follows:

$$G=a_1H_1 \smile a_2H_2 \cdots \smile a_{n-1}H_{n-1} + \cdots d_1H_1 \smile d_2H_2 \cdots \smile d_{n-1}H_{n-1} + X.$$

And let the decomposition of G by cosets with respect to H_n be as follows.

$$G=(a_nH_n+b_nH_n+\cdots+d_nH_n)+(pa_nH_n+qb_nH_n+\cdots+sd_nH_n)+\cdots.$$

The set

$$G-(a_1H_1 \smile \cdots \smile a_{n-1}H_{n-1} + \cdots + d_1H_1 \smile \cdots \smile d_{n-1}H_{n-1})=G-Q$$

is contained in the set $(a_nH_n+\cdots+d_nH_n)$. So, $(pa_nH_n+\cdots+sd_nH_n)$ is contained in the set Q. Therefore, G is covered by $Q+p^{-1}Q+\cdots+s^{-1}Q$. This contradicts with the assumption that G has not a finite covering of union-cosets of degree $n-1$.

THEOREM 3. *A division algebra D is generated by two elements over the center, and one of them is separable over the center.*

Proof. A division algebra D has a separable maximal subfield M over the center Z, and there exist only a finite number of subfields in M over Z. By lemma 5, D can not be covered by their commutator algebras. Therefore, there exists an element β such that $M(\beta)=D$. So, D is generated by two elements over Z, and one of them is separable over Z.

THEOREM 4. *Let D be a division algebra with center Z and β be any element of D not in Z, then there exists a separable element over Z such that $Z(\alpha, \beta)=D$.*

Proof. Let M be a separable maximal subfield of D, then there are a finite number of subfields betwien M and Z. These subfields are simple extensions over Z. Let $\gamma_1, \gamma_2, \cdots, \gamma_l$ be generating elements of these subfields over Z. By lemma 5, there exists an element b which does not lie in any commutater algebras of $\gamma_1, \gamma_2, \cdots, \gamma_l$ and $V_D(\beta)$. But, Nagahara's lemma says that for γ and $V_D(\beta)$, in the set of elements $b+c_1, b+c_2, \cdots, c_i \in Z$, there exist at most two $(b+c_i)$'s which transform γ into $V_D(\beta)$. So, there exists an element t transforming all subfields of M over Z out of $V_D(\beta)$. Therefore, $V_D(\beta)\frown t^{-1}Mt=Z$, and $t^{-1}Mt(\beta)$ becomes D.

4. Normality in a division algebra *D*.

Let D be a division algebra with center Z and A a division subalgebra of D such that D is Galois over A. Then by theorem 2, D is Galois over $A\frown Z=Z_0$. Consequently, Galois conditions are as follows:

1) Z is separable, finite and normal over Z_0 and
2) D is $\bar{G}$-normal over $Z_0=A\frown Z$, that is, every automorphism of $\bar{G}$ can be extended to an automorphism in D, where $\bar{G}$ is the Galois group of Z/Z_0.

First we consider the normality in commutative cases. Let N be a finite extension field of Z, and Z_0 be a subfield of Z such that Z is Galois over Z_0. Let $\bar{\sigma}$ be an automorphism of Z/Z_0. The conditions of $\bar{G}$-normality are as follows:

1) N is separable over Z and
2) If every polynomial $g(x)$, irreducible in $Z[x]$, has one root α in N, then the conjugate polynomial $g^{\bar{\sigma}}(x)$ has one root α' in N.

Let α be a generating element of N over Z, and $f(x)=0$ be the defining equation of α over Z_0, then $f(x)$ is decomposed into conjugate prime factors of the same degree with respect to Z/Z_0:

$$f(x)=f_0(x)\cdots f_0^{\bar{\sigma}}(x).$$

If $f_0(\alpha)=0$, then from 1), there is an element α' such fact $f_0^{\bar{\sigma}}(\alpha')=0$. The mapping

$$\alpha\to\alpha', \qquad Z\to Z^{\bar{\sigma}}.$$

is an automorphism in N.

These conditions can be written in language of ideal as follows. If every ideal in the polynomial ring $Z[x]$ has one root α in N, then the conjugate ideal with respect to Z/Z_0 has one root α' in D, where a root of ideal is an element which is a root of all polynomials of the ideal.

In the preceding paragraph we see that a division algebra is generated by two elements (α, β) over the center Z. And any element d of D is represented by a non-commutative polynomial in (α, β). For, non-zero element d in D has the inverse element in D and from finite dimensionality the inverse element is represented by a polynomial in d. Therefore, the polynomial ring $Z[\alpha, \beta]$ becomes D itself.

Thus, if we denote by $Z[x, y]$ the non-commutative polynomial ring, then $Z[x, y]$ may be mapped homomorphically upon $Z[\alpha, \beta]=D$. The homomorphism is given by the following mapping:

$x \rightarrow \alpha$, $y \rightarrow \beta$. Elements of Z are invariant.

So, let $f(x, y)$ be an element of $Z[x, y]$:

$$f(x, y)=\sum_{i=1}^{l} a_i[x, y]_i,$$

where $[x, y]_i$ are free products of x, y and $a_i \in Z$.
Then, the homomorphic image of $f(x, y)$ is represented by

$$f(\alpha, \beta)=\sum_{i=1}^{l} a_i[\alpha, \beta]_i.$$

The kernel of this homomorphism is two-sided ideal $\mathfrak{p}$ of all polynomials $f(x, y)$ which have (α, β) as roots, i.e., for which $f(\alpha, \beta)=0$. And,

$$Z[x, y]/\mathfrak{p} \cong Z[\alpha, \beta]=D.$$

From the structure of D, the ideal $\mathfrak{p}$ has the following properties:
1) if $ab \equiv 0 \pmod{\mathfrak{p}}$, then $a \equiv 0$ or $b \equiv 0 \pmod{\mathfrak{p}}$,
2) $Z[x, y]$ has a finite basis over Z mod $\mathfrak{p}$.

$$[Z[x, y]/\mathfrak{p} : Z]=[D : Z]=n^2,$$

3) the center of $Z[x, y]/\mathfrak{p}$ is Z.

When an ideal $\mathfrak{p}$ in $Z[x, y]$ has the properties 1)–3), we say that $\mathfrak{p}$ is an R-ideal of degree n^2.

Conversely, if $\mathfrak{p}$ is an R-ideal of degree n^2, then $Z[x, y]/\mathfrak{p}$ becomes a division algebra with center Z. For, let $a \not\equiv 0 \pmod{\mathfrak{p}}$, then by 2), there is an irreducible polynomial $f(x)$ in $Z[x]$ such that $f(a) \equiv 0 \pmod{\mathfrak{p}}$. By 1), the constant term can not be zero. So, a has the inverse element in $Z[x, y]$ mod $\mathfrak{p}$) and $Z[x, y] \pmod{\mathfrak{p}}$ is a division algebra of degree n^2 with center Z.

From 1)–3), if (α, β) are roots of $\mathfrak{p}$, then the root ideal of (α, β), that is, the set of all polynomials which have (α, β) as roots, does not distinct from $\mathfrak{p}$. For, let $f(x, y)$ be a polynomial such that $f(\alpha, \beta)=0$ but not in $\mathfrak{p}$, then $f(x, y)$ has the inverse polynomial $g(x, y) \pmod{\mathfrak{p}}$:

$$f(x, y)g(x, y) \equiv 1 \pmod{\mathfrak{p}}.$$

Then we obtain

$$f(\alpha, \beta)g(\alpha, \beta)=0=1.$$

This is a contradiction.

Let $\bar{\sigma}$ be an automorphism of the center Z/Z_0, then $\bar{\sigma}$ can be extended to an automorphism σ of $Z[x, y]$ by the following correspondence:

$$f(x, y)=\sum_{i=1}^{l}a_i[x, y]_i \rightarrow f^{\sigma}(x, y)=\sum_{i=1}^{l}a_i^{\bar{\sigma}}[x, y]_i.$$

By the automorphism σ, an R-ideal $\mathfrak{p}$ is mapped onto $\mathfrak{p}^{\sigma}$ which is the set of all conjugate polynomials $f^{\sigma}(x, y)$ of $f(x, y)$ in $\mathfrak{p}$. Then $\mathfrak{p}^{\sigma}$ has the properties 1)–3). For,

1) if $f^{\sigma}(x, y)g^{\sigma}(x, y)\equiv 0 \pmod{\mathfrak{p}}$, then $f(x, y)g(x, y)\equiv 0 \pmod{\mathfrak{p}}$ and by 1) of $\mathfrak{p}$, $f(x, y)\equiv 0$ or $g(x, y)\equiv 0 \pmod{\mathfrak{p}}$.
2) let $u_1, u_2, \cdots, u_{n^2}$ be linearly independent polynomials in $Z[x, y] \pmod{\mathfrak{p}}$, then $u_1^{\sigma}, u_2^{\sigma}, \cdots, u_{n^2}^{\sigma}$ are linearly independent over Z (mon $\mathfrak{p}^{\sigma}$). So, the dimension of $Z[x, y] \pmod{\mathfrak{p}^{\sigma}}$ over Z is invariant by σ.
3) if $f^{\sigma}(x, y)$ be contained in the center of $Z[x, y] \pmod{\mathfrak{p}}$, then

$$f^{\sigma}(x, y)x\equiv xf^{\sigma}(x, y) \pmod{\mathfrak{p}^{\sigma}},$$

$$f^{\sigma}(x, g)y\equiv yf^{\sigma}(x, y) \pmod{\mathfrak{p}^{\sigma}}.$$

Therefore, $f(x, y)$ is contained in Z mod $\mathfrak{p}$. So, $f^{\sigma}(x, y)$ lies in $Z \pmod{\mathfrak{p}^{\sigma}}$.

Now we can define the normality in a division algebra D with center Z which is Galois over its subfield Z_0 as follows:

DEFINITION. D is said to be *$\bar{\mathfrak{G}}$-normal with respect to Z/Z_0* if an R-ideal $\mathfrak{p}$ in $Z[x, y]$ has roots (α, β) in D, then the conjugate R-ideal $\mathfrak{p}^{\sigma}$ with respect to Z/Z_0 has roots (α', β') in D, where $Z[x, y]$ is the ring of all non-commutative polynomials of (x, y) with coefficient in Z.

This definition is a natural extension of that of commutative cases. If this condition is satisfied in D, then D is Galois over Z.

Let (α, β) be generating elements of D over Z: $D=Z[\alpha, \beta]$. Let $Z[x, y]$ and the kernel of the homomorphism is an R-ideal $\mathfrak{p}$. Let $\bar{\sigma}$ be an automorphism of Z leaving the elements Z_0 invariant, then by the preceding assertion $\bar{\sigma}$ can be extended to an automorphism σ of $Z[x, y]$. And the R-ideal $\mathfrak{p}$ is mapped upon $\mathfrak{p}^{\sigma}$ which has the properties 1)–3). Therefore, $Z[\alpha', \beta']$ becomes D and the mapping:

$$\alpha\rightarrow\alpha', \qquad \beta\rightarrow\beta'$$

is an automorphism in D. So, by Jacobson-Teichwüller's conditions, D is Galois over Z_0.

Conversely, when D is Galois over Z_0, and let an R-ideal $\mathfrak{p}$ of $Z[x, y]$ has roots (α, β) in D, then by automorphisms σ of D leaving the elements of Z_0 invariant, $Z[\alpha, \beta]$ is mapped onto $Z^{\sigma}[\alpha^{\sigma}, \beta^{\sigma}]$ and $(\alpha^{\sigma}, \beta^{\sigma})$ are roots of conjugated R-ideal $\mathfrak{p}^{\sigma}$ with respect to Z/Z_0.

Consequently, we obtain the following theorem.

THEOREM 5. *A division algebra D with center Z is Galois over its division subalgebra A if, and only if,* 1) *Z is Galois over $A\frown Z$ and* 2) *D is $\bar{\mathfrak{G}}$-normal with respect to $Z/A\frown Z$.*

REFERENCES

[1] ALBERT, A. A., Two elements generation of a separable algebra. Bull. Amer. Math. Soc. 50 (1944), 786–788.

[2] ARTIN, E., Galois theory. Notre Dame, (1942).
[3] ARTIN, E., C. NESBITT, AND R. THRALL, Rings with minimum condition. University of Michigan, (1944).
[4] BRAUER, R., On a theorem of H. Cartan. Bull. Amer. Math. Soc. **55** (1949), 619–620.
[5] EILENBERG, S., AND S. MACLANE, Cohomology and Galois theory, 1. Trans. Amer. Math. Soc. **64** (1948), 1–20.
[6] FAITH, C. C., On conjugates in division rings. Canad. J. Math. **10** (1958), 374–380.
[7] JACOBSON, N., A note on division rings. Amer. J. Math. **64** (1947), 27–36.
[8] KASCH, F., Über den Satz vom primitiven Element bei Schiefkörpern. J. Reine Angew. Math. **189** (1951), 150–159.
[9] MCCOY, N. H., Prime ideals in general rings. Amer. J. Math. **71** (1949), 823–833.
[10] NAGAHARA, T., On generating elements of Galois extensions of division rings. Math. J. Okayama Univ. **6** (1957), 181–190.
[11] OKUZUMI, M., Generating elements in a field. Kōdai Math. Sem. Rep. **16** (1964), 127–128.
[12] TEICHMÜLLER, O., Über die sogenannte nichtkommutative Galoissche Theorie. Deutsche Math. **5** (1940), 138–149.
[13] TOMINAGA, H., On right regular rings. Proc. Japan Acad. **29** (1953), 486–489.

TRAINING INSTITUTE FOR ENGINEERING TEACHERS,
TOKYO INSTITUTE OF TECHNOLOGY.