On algebraic Galois extensions of simple rings

Takasi Nagahara*
ON ALGEBRAIC GALOIS EXTENSIONS
OF SIMPLE RINGS

TAKASI NAGAHARA*

Throughout the present paper, $R$ will be a simple ring, $S$ a simple
subring of $R$ (with common 1). And $V$, $C$, and $Z$ represent $V_b(S)$, $V_n(R)$
and $V_b(S)$ respectively. If $M$ is a unitary $R$-left (right) module, $[M|R]$,
($[M|R]_r$) will denote the uniquely determined number (finite or infinite)
of irreducible direct summands of $M$. When $R$ is Galois over $S$, we denote
by $\Theta$ the Galois group of $R/S$. And, as to notations and terminologies used
in this paper, we follow the previous one [4]. The writer is grateful to
Dr. H. Tominaga for his kind advices.

In case $R$ is a division ring, we proved that if $R$ is Galois, left algebraic
and of bounded degree over a division subring $S$ then $R$ is finite over
$S$ [3, Theorem 4]. Afterwards, in case $S$ is a central simple algebra of
finite rank, this result has been extended to simple rings [4, Theorem
5.2]. One of the purposes of this paper is to present the complete extension
of [3, Theorem 4] to simple rings:

**Theorem 1.** If $R$ is Galois, left algebraic and of bounded degree
over $S$ then $R$ is finite over $S$.

Next, we shall prove a theorem which is a partial extension of [3,
Theorem 3] and [4, Theorem 5.1]:

**Theorem 2.** If $R$ is Galois and left algebraic over $S$ then $R$ is locally
finite over $S$, provided the Galois group $\Theta$ of $R/S$ is almost outer,
(whence $
\Theta$ is locally finite).

For the proofs of our principal theorems, several lemmas will be
needed. At first we shall prove the following:

**Lemma 1.** Let $S$ be a division subring of $R$. $N$ a $Z$-right submodule
of $R$ with $[N:Z] < \infty$. If $[S:Z] = \infty$ then for each positive integer $q$
there exist $q$ non-zero elements $s_1, \ldots, s_q \in S$ such that $\sum_1^q N s_i = \sum_1^q \Theta^i_N$.

**Proof.** Patterning after the latter half of the proof of [4, Lemma 6.6]
or the proof of [2, Lemma 3] according as $S$ is algebraic or transcendental
over $Z$ ($V$ should be replaced by $Z$), one will easily obtain our lemma.
And so, the details may be left to readers.

**Lemma 2.** Let $R/S$ be Galois, $S'$ an intermediate ring of $R/S$ such

---

* Yukawa Fellow of Osaka University in 1961.
that \( R \) is \( S'-R \)-irreducible, and let \( M \neq 0 \) be an \( S-S' \)-submodule of \( R \).

(i) \((\sigma | M) R_r \) is \( S'-R \)-irreducible and \( R_r \)-isomorphic to \( R_r \) for each \( \sigma \in \mathfrak{S} \).

(ii) For any subset \( \mathfrak{B} \) of \( \mathfrak{S} | M \), \( \mathfrak{B} \) is linearly independent over \( R_r \) if and only if so it is over \( V_r \).

(iii) \((\mathfrak{S} | M) R_r \) possesses a subset of \( \mathfrak{S} | M \) as a linearly independent \( R_r \)-basis, and \( \mathfrak{B} \subseteq \mathfrak{S} | M \) is a linearly independent \( R_r \)-basis of \((\mathfrak{S} | M) R_r \) if and only if it is a linearly independent \( V_r \)-basis of \((\mathfrak{S} | M) V_r \).

Proof. (i) Let \( x \) be an arbitrary non-zero element of \( R \). Then, by our assumption, there holds \( S' \langle \sigma | M \rangle x_r R_r = (\sigma | M) \langle S' \sigma x R \rangle_r = (\sigma | M) \langle (S' x \sigma^{-1} R) \sigma \rangle_r = (\sigma | M) R_r \), whence our assertion is clear.

(ii) Let a subset \( \mathfrak{B} \) of \( \mathfrak{S} | M \) be linearly dependent over \( R_r \), and let \( \sum_{i=1}^{s} (\sigma_i | M) x_{i} = 0 \) (\( x_i \in R \)) be a non-trivial relation of the shortest length. Then, by (i), we obtain \( \sigma_i | M = \sum_{j=1}^{s} (\sigma_i | M) y_{i} \) for some \( y_i \in R \). Here, by making use of the standard argument, one can easily see that each \( y_i \) is contained in \( V \). Hence, we have proved that \( \mathfrak{B} \) is linearly dependent over \( V_r \). And the converse is trivial.

(iii) This is an easy consequence of (i) and (ii).

By the validity of Lemma 2, we can prove the following useful inequalities.

Lemma 3. Let \( R/S \) be Galois, and \( S' \) an intermediate ring of \( R/S \) such that \( R \) is \( S'-R \)-irreducible. If \( M \) is an \( S-S' \)-submodule of \( R \) with \([M:S]_t < \infty \) then for each \( a \in M \) there holds

\[
m \cdot [a \mathfrak{S} | V_r : V_r]_r < mm' + m' \cdot [M:S]_t,
\]

where \( m = [S:S] \) and \( m' = [V:V] \) are the capacities of \( S \) and \( V \) respectively. In particular, if \( S \) is a division ring, we have

\[
\frac{1}{m'} [a \mathfrak{S} | V_r : V_r]_r < 1 + [M:S]_t.
\]

Proof. By Lemma 2 (i) and (ii), there holds

\[
m \cdot [a \mathfrak{S} V_r : V_r]_r \leq m \cdot [((\mathfrak{S} | M) V_r : V_r]_r = mm' \cdot [((\mathfrak{S} | M) V_r : V_r]_r = mm' \cdot [((\mathfrak{S} | M) R_r : R_r]_r.\]

Thus, to complete our proof, it suffices to prove the next:

\[
m \cdot [((\mathfrak{S} | M) R_r : R_r]_r < m + [M:S]_t.
\]

Now, we can find a \( S \)-left submodule \( M' \) of \( R \) such that \([M':S]_t < m\), \( M^* = M + M' = M \oplus M' \), and that \( M^* \) possesses a linearly independent \( S \)-left basis. Then, by Lemma 2 (i), we obtain

\[
[M^*:S]_t = [\text{Hom}_S(M^*, R) : R_r]_t \geq [((\mathfrak{S} | M) R_r : R_r]_t.
\]

Consequently, there holds \([M|S]_t + m > [M|S]_t + [M'|S]_t \geq \)

http://escholarship.lib.okayama-u.ac.jp/mjou/vol11/iss1/6
ON ALGEBRAIC GALOIS EXTENSIONS

Now, we shall prove the following lemma which will play an essential role in our present study.

**Lemma 4.** If $R/S$ is Galois, left algebraic and of bounded degree then $[R:S] < \infty$, provided there exists an intermediate ring $S'$ of $R/S$ with $[S':S] < \infty$ such that $R$ is $S'$-irreducible.

**Proof.** At first, we shall remark that $V$ is finite over $Z$. For, noting that $S[V] = S \times_Z V$, we readily see that $V$ is an algebraic algebra over $Z$ and of bounded degree, and so $[V:V_r(V)] < \infty$ by [1, Theorem 7.11.1]. Moreover, $V/Z$ being Galois, it will be easy to see that $V_r(V)$ is finite over $Z$. Hence, it follows $[V:Z] < \infty$.

Let $S = \sum_{j=1}^r S_j f_{ij}$ where $f_{ij}$'s are matrix units and $S_0 = V_s(\{f_{ij}\})$ is a division ring. Then, as is well-known, $S' = \sum_{j=1}^r S'_j f_{ij}$ and $R = \sum_{j=1}^r R_j f_{ij}$ for $S'_j = V_s(\{f_{ij}\})$ and the simple ring $R_0 = V_s(\{f_{ij}\})$. Here, one will easily see that $R_0/S_0$ is Galois, left algebraic and of bounded degree, and that $R$ is $S'_0$-irreducible. Further, our assertion for the case $[S:Z] < \infty$ has been proved in [4, Theorem 5.2]. Thus, in what follows, we may, and shall, restrict our proof to the case where $S$ is a division ring and $[S:Z] = \infty$.

Let $S' = S u_1 + \cdots + S u_p$, and $s = \max_{s \in R} |(S[x] : S)|$. And let $t$ be an integer such that $t \geq 1 + ps$. Now, we suppose that $[R:S] = \infty$. As, to be easily verified, $\Theta R_r$ is two-sided simple, if $[\Theta R_r : R]_r < \infty$ then one can easily see that $[R:S] < \infty$. This contradiction shows that $[\Theta R_r : R]_r = \infty$. And so, there exist some $\alpha, \beta, \gamma, \in \Theta$ such that $\{\alpha, \beta, \gamma\}$ is linearly independent over $R$. If $x$ is an element of $R$, $S x S' = S x (S u_1 + \cdots + S u_p) \subseteq S[x] u_1 + \cdots + S[x] u_p$ yields

\[(1) \quad [S x S': S]_r \leq sp.\]

Here, choose an arbitrary $S-S'$-submodule $M_0$ of $R$ with $[M_0 : S] < \infty$. If $\sum_{i=1}^{n_1} (\sigma_i | M_0) R : R_0 < t$ (cf. Lemma 2 (i)), then there holds a non-trivial relation: $\sum_{i=1}^{n_1} (\sigma_i | M_0) a_{rv} = 0$ ($a_{rv} \in R$). Since $\sigma = \sum_{i=1}^{n_1} \sigma_i a_{rv} \neq 0$, there exists some $b_1 \in R$ such that $b_1 v \neq 0$. We set here $M_1 = M_0 + S b_1 S'$. Then, by (1) we have $[M_1 : S]_r < \infty$. And $M_0 \alpha \neq 0$ implies $[\sum_{i=1}^{n_1} (\sigma_i | M_0) R : R]_r < [\sum_{i=1}^{n_1} (\sigma_i | M_0) R : R]_r$. Thus, repeating the same procedures, we can find eventually an $S-S'$-submodule $M = S d_1 + \cdots + S d_s$ of $R$ such that $t = [\sum_{i=1}^{n_1} (\sigma_i | M) R : R]_r$. Recalling the fact $[V:Z] < \infty$ remarked at the opening, we see that $N = \sum_{i=1}^{n_1} (d_i | N) V$ is right-finite over $Z$. And so, by Lemma 1, there exist some non-zero $s_0, \cdots, s_n \in S$ such that

\[(2) \quad \sum_{j=1}^{n_1} N s_j = \sum_{j=1}^{n_1} \bigoplus N s_j.\]
We set here \( a = \sum_j s_j d_j s_j \) (\( \in M \)). If \( \sum_{j=1}^q (a\sigma) v_i = 0 \) (\( v_i \in V \)), then \( \sum_{j=1}^q (d_j\alpha^j) s_j = \alpha^j = \sum_{j=1}^q (a\sigma) v_i = 0 \), where \( \alpha^j = \sum_{j=1}^q (\sigma_j | M) v_i \). Noting that \( d_j\alpha^j \in N \), there holds \( d_j\alpha^j = 0 \) (\( j = 1, \cdots, q \)) by (2). And this implies \( \mathcal{M}\alpha' = \sum_{j=1}^q \delta_j (d_j\alpha^j) = 0 \), that is, \( 0 = \alpha' = \sum_{j=1}^q (\sigma_j | M) v_i \). Since \( \{ \sigma_j | M, \cdots, \sigma_j | M \} \) is linearly independent over \( V \), we have \( v_i = 0 \) (\( i = 1, \cdots, t \)). We have proved therefore that \( a\sigma, \cdots, a\sigma \) is linearly independent over \( V \). Accordingly, by (1) and Lemma 3 we obtain

\[
1 + ps \geq 1 + [SaS' : S] \geq \frac{1}{m'} [a\mathcal{M}V : V], \geq [\sum_{j=1}^q (a\sigma) v_i : V], = t,
\]

where \( m' \) is the capacity of \( V \). But this contradicts \( t \geq 1 + ps \), and our proof is complete.

**Lemma 5.** Let \( R/S \) be Galois and left algebraic. If \( \mathcal{O} \) is almost outer and \( S' \) is an intermediate ring of \( R/S \) with \( [S' : S] : \infty \) such that \( R \) is \( S'-\text{irreducible} \) then for each \( x \in S' \) we have \( \# \{ x\mathcal{O} \} < \infty \).

**Proof.** Since \( \mathcal{O} \) is almost outer, i.e. \( (V^* : C^*) \) (the group index of the multiplicative group \( C^* \) of non-zero elements of \( C \) in the multiplicative group \( V^* \) of regular elements of \( V \)) \( < \infty \), \( V \) is finite or \( V = C \) by [6, Lemma 1]. In virtue of Lemma 2 (i), we have

\[
[\mathcal{O} | S'] R = \sum_{j=1}^q (\sigma_j | S') R, \text{ with some } \sigma_j \in \mathcal{O}.
\]

Then, by Lemma 2 (iii), \( \{ \sigma_j | S', \cdots, \sigma_j | S' \} \) is a linearly independent \( V_r \)-basis of \( \mathcal{O} \). Hence, \( \{x\sigma \} \) \( \mathcal{O} \)-basis. Thus, in what follows, we may, and shall, restrict our proof to the case \( V = C \). Now, let \( \sigma \) be an arbitrary element of \( \mathcal{O} \). Then \( \sigma | S' = \sum_{j=1}^q (\sigma_j | S') v_i \), (\( v_i \in V \)). And so, each \( x \in S' \) we have

\[
x_\sigma (x \sigma) = \sum_{j=1}^q (\sigma_j | S') (x \sigma) v_i = \sum_{j=1}^q (\sigma_j | S') (x \sigma) v_i.
\]

Hence, we obtain \( \sum_{j=1}^q (\sigma_j | S') (x \sigma) v_i = 0 \), whence it follows \( (x \sigma - x \sigma) v_i = 0 \). Noting that some of \( v_i \)'s, say \( v_i \), is non-zero, we see that \( x \sigma = x \sigma \). We have proved therefore that \( x \mathcal{O} = \{ x \sigma, \cdots, x \sigma \} \).

Now, let \( R \) be represented as \( \sum_{i=1}^n D e_i \) with matrix units \( e_i \)'s and a division ring \( D = V_R (\{ e_i \}) \). If \( n > 1 \) and \( S \) contains an element \( a = \sum_{i=1}^n c_i e_i \) with \( c_{ps} \neq 0 \) for some \( p \neq q \) then, for an arbitrary permutation

\[
\begin{pmatrix}
1 & 2 & \cdots & n-1 & n \\
\vdots & \ddots & \ddots & \vdots & \vdots \\
p_1 & p_2 & \cdots & p_{n-1} & p_n
\end{pmatrix}
\]

\[
1) \text{For any } E, \#(E) \text{ will signify the cardinal number of } E.
\]
such that \( p_1 = p \) and \( p_n = q \). \( e'_{ij} = e_{p_ip_j} \) can be adopted as new matrix units of \( R \) and \( e'_{in} = e_{pn} \). Accordingly, without loss of generality, we may assume that \( c_{in} \neq 0 \). On the other hand, if \( n > 1 \) and every element of \( S \) is diagonal, it is clear that all \( e_{it} \in V \). Hence, \( V = \sum_{i=1}^{n} e_{ii} V \). If moreover \( V \) is a simple ring, the last fact means \( [V : V] \leq [R : R] \). Since \( [V : V] \leq [R : R] \) trivially, \( [V : V] = [R : R] \). Accordingly, if \( V = \sum_{i,j=1}^{n} e_{ij} e'_{ij} \) with matrix units \( e'_{ij} \)'s and a division ring \( E' = V_r(\{ e'_{ij} \}'s) \), then \( R = \sum_{i,j=1}^{n} D' e'_{ij} \) with the division ring \( D' = V_r(\{ e'_{ij} \}'s) \). Thus, to prove our principal theorems, it will suffice to restrict our subsequent consideration to the following three cases:

Case I. \( n = 1 \).

Case II. \( n > 1 \) and \( S \) contains an element \( a = \sum_{i=1}^{n} c_{ij} e_{ij} \) with \( c_{in} \neq 0 \).

Case III. \( n > 1 \) and \( S \subseteq D \).

Lemma 6. Let Case II happen.

(i) Let \( \begin{pmatrix} 1 & 2 & \cdots & n-1 & n \\ p_1 & p_2 & \cdots & p_{n-1} & p_n \end{pmatrix} \) be an arbitrary permutation such that \( p_1 = 1 \) and \( p_n = n \), and \( x_1, x_2, \ldots, x_n \) arbitrary non-zero elements of \( D \). If \( r = \sum_{t=1}^{n} x_t e_{p_1p_{t-1}} \) then \( R \) is \( S[r] \)-R-irreducible.

(ii) If \( D \neq GF(2) \) then \( R = S[F] \), where \( F \) is the set of elements \( R \) such that \( R \) is \( S[r] \)-R-irreducible.

Proof. (i) If we set \( e'_{ij} = e_{p_ip_j} \) then \( e'_{in} = e_{in} \) and \( r = \sum_{i=2}^{n} x_i e'_{ii-1} \). And so, without loss of generality, we may assume that the permutation is identical. Let \( M \) be an arbitrary non-zero \( S[r] \)-R-submodule. Then, \( M \) contains an element \( b = \sum_{i=1}^{n} d_i e_{ii} \) with \( d_i \neq 0 \) for some \( p \). Since \( M \ni r^{n-p}b = x_n \cdots x_{p-1}d_p e_{pn} \) (if \( p = n \), \( M \ni b = d_n e_{nn} \)), \( e_{nn} \) is contained in \( M \), whence it follows \( M \ni ae_{nn} = \sum_{i=1}^{n} c_{ii} e_{ii} \). Hence, there holds \( M \ni r^{n-k} \sum_{i=1}^{n} e_{ii} = x_n e_{nn} + x_{n-1} e_{n(n-1)} + \cdots + x_{k+1} e_{k(k+1)} + x_{k} e_{k(k-1)} + \cdots + x_1 e_{12} \) (\( k = 1, \ldots, n \)). Recalling that \( c_{in} \neq 0 \), one can see inductively that \( e_{nn}, e_{n-1n}, \ldots, e_{12} \in M \), whence eventually \( e_{ij} \in M \). Now, it will be easy to see that \( M = R \).

(ii) Let \( \begin{pmatrix} 1 & 2 & \cdots & n-1 & n \\ p_1 & p_2 & \cdots & p_{n-1} & p_n \end{pmatrix} \) be an arbitrary permutation such that \( p_1 = 1 \) and \( p_n = n \), and let \( x \) be an arbitrary non-zero element of \( D \). Then, by (i) \( F \ni r_{x,t} = e_{p_ip_{n-1}} + \cdots + xe_{p_ip_{t-1}} + \cdots + e_{p_ip_1} \) (\( 2 \leq i \leq n \)). Since there exists an element \( z \in D \) different from 1 and 0, \( S[F] \ni r_{z,t} - r_{z-1,t} = e_{p_ip_{t-1}} \) (\( 2 \leq i \leq n \)). Further for arbitrary \( y \in D \) different from 1 and 0 we obtain \( S[F] \ni r_{1,t} - r_{1-x,t} = ye_{p_ip_{t-1}} \) (\( 2 \leq i \leq n \)). Hence, noting that \( xe_{ij} = xe_{i-1e_{i-1}} + \cdots + e_{ii} \), we see that \( S[F] \ni De_{nj} \) (\( 1 \leq j < n \)), \( De_{ij} \) (\( 1 < i \neq j < n \)) and \( De_{ii} \) (\( 1 < i \leq n \)). Consequently,
(3) \[ S[F] \equiv (\sum_{i,j=0}^{n} c_{ij}e_{ij})c_{nn}^{-1}xe_{nk} \]

\[ = c_{nn}^{-1}xe_{nk} + \sum_{i=0}^{n-1} c_{in}c_{nn}^{-1}xe_{ik} + xe_{ik} \quad (1 \leq k < n). \]

Since for \( n > k > 1 \) \( S[F] \) contains \( e_{kl}(\sum_{i,j=0}^{n} c_{ij}e_{ij})c_{nn}^{-1}de_{nk} = de_{nk}(d \in D) \), it will be easily seen that \( S[F] \supseteq \sum_{i=0}^{n-1} c_{in}c_{nn}^{-1}xe_{ik} \). Hence, from (3), we obtain \( xe_{ik} \in S[F] \) (1 \( \leq k < n \)), in particular, \( e_{11} \in S[F] \). And so, \( S[F] \) contains \( e_{nn} = 1 - \sum_{i=1}^{n-1} e_{ii}e_{11} \) too; whence it follows \( e_{nn} = c_{nn}^{-1}e_{11}(\sum_{i,j=0}^{n} c_{ij}e_{ij})e_{nn} \in S[F] \).

Thus, we have proved that \( e_{ij} \in S[F] \) (1 \( \leq i \leq n \), \( i \neq j \)), \( e_{ij} \in S[F] \) and \( D \subseteq S[F] \).

\textbf{Lemma 7.} Let Case III happen, \( R/S \) be left algebraic and \( S \nsubseteq C \) (whence \( D \subseteq V \) by \( D \nsubseteq S \)).

(i) For an arbitrary \( x \in D \setminus V \), if \( r = \sum_{i=1}^{n} x_{ii} + xe_{11} \) then \( R \) is \( S[r] \)-R-irreducible.

(ii) \( R = S[F] \), where \( F \) is the set mentioned in Lemma 6 (ii).

\textbf{Proof.} (i) There exists an element \( y \in S \) with \( xy \neq yx \). Since \( r^{-1} = \sum_{i=1}^{n} x_{ii}e_{ii} + x^{-1}e_{11} \in S[r] \), \( S[r] \) contains \( r^{-1}(r - yry^{-1})(r^{-1} - yry^{-1})y^{n-1} = (x - yxy^{-1})(x^{-1} - yx^{-1}y^{-1})e_{11} \). Noting that \( (x - yxy^{-1})(x^{-1} - yx^{-1}y^{-1}) \) is a non-zero element of \( S[r] \cap D \), it follows \( e_{ij} \in S[r] \) (\( i, j = 1, \ldots, n \)). Now the \( S[r] \)-R-irreducibility of \( R \) will be easy.

(ii) By (i), it is clear that \( e_{ij} \) (\( i, j = 1, \ldots, n \)) and arbitrary \( x \in D \setminus V \) are contained in \( S[F] \) (and so \( x^{-1} \in S[F] \) as well). On the other hand, if \( c \) is a non-zero element of \( D \setminus V \) then \( xc \in S[F] \) for arbitrary \( x \in D \setminus V \), whence it follows \( c \in S[F] \). Consequently, we obtain \( R = \sum_{i,j=1}^{n} Dc_{ij} = S[F] \).

Now we can prove our principal theorems.

\textbf{Proof of Theorem 1.} For Case I, \( R \) being \( S \)-R-irreducible, our assertion is a direct consequence of Lemma 4. Next, for Case II it is easy by Lemma 6 (i) and Lemma 4. And finally, our assertion for Case III is contained in [4, Theorem 5.2] provided \( S \subseteq C \), and for the case remained it is clear by Lemma 7 (i) and Lemma 4.

\textbf{Proof of Theorem 2.} If \( D = GF(2) \), our assertion is trivial. For case 1, noting that \( R \) is always \( S[r] \)-R-irreducible for \( r \in R \), \( \mathbb{S} \) is locally finite by Lemma 5. Similarly, for Case II and Case III, by making respective use of Lemma 6 and Lemma 7 together with Lemma 5 we see that \( \mathbb{S} \) is locally finite provided \( D \neq GF(2) \) and \( S \nsubseteq C \) respectively. Finally, if \( n > 1 \) and \( S \subseteq C \) then \( V = R \) is finite by [6, Lemma 1] (for, \( \mathbb{S} \) is almost outer).

From Lemma 5, Theorem 2 and [5, Theorem 1.1 and Theorem 3.1] we obtain the following:

\textbf{Corollary 1.} If \( R/S \) is left algebraic and outer Galois then, for any finite subset \( E \) of \( R \),
(i) $\#(E\mathfrak{g})$ is finite,
(ii) the ring $S[E]$ generated by $E$ over $S$ is a simple ring which is finite over $S$,

By Corollary 1, it will be easy to see that the infinite Galois theory of division rings [1, VII, § 6] of N. Jacobson can be extended to simple rings under the same assumptions such that $R/S$ is left algebraic and outer Galois as in [1, VII, § 6]. The following corollary is one of those extensions.

**Corollary 2.** If $R/S$ is left algebraic and outer Galois then there exists a 1–1 dual correspondence between closed subgroups of $\mathfrak{g}$ and intermediate rings of $R/S$, in the usual sense of Galois theory.

**References**


**Department of Mathematics, Okayama University.**

(Received January 24, 1962)

---

2) This is a restatement of the latter part of [4, Corollary 1, 4].