GALOIS THEORY
OF
SIMPLE RINGS

BY

Hisao TOMINAGA and Takasi NAGAHARA
Department of Mathematics
Okayama University, Japan

1970

OKAYAMA MATHEMATICAL LECTURES

GALOIS THEORY
OF
SIMPLE RINGS

BY

HISAO TOMINAGA and TAKASI NAGAHARA
Department of Mathematics
Okayama University, Japan

1970

Preface

One of the most essential and beautiful principles in mathematics is of duality, and its typical representative can be found in the Galois theory of fields. Since the Galois theory of equations was seized by E. Steinitz as the Galois theory of fields, the finite dimensional Galois theory of rings has been extensively making progress, and the Galois theory of division rings independently due to H. Cartan and N. Jacobson may be viewed as the new starting point of its development. Thereafter, the theory was extended to simple ring and other ring extensions of finite dimension mainly by G. Hochschild, T. Nakayama, G. Azumaya, J. Dieudonné, A. Rosenberg and D. Zelinsky, and further contributions were made by F. Kasch, S. A. Amitsur, C. C. Faith and the authors. On the other hand, W. Krull gave the Galois theory for infinite dimensional algebraic field extensions, which produced a telling influence on the modern number theory. In the last decade, at first N. Jacobson and N. Nobusawa tried independently to extend Krull's theory to division rings and then, passing through the sequential investigation, the authors have succeeded in constructing a unified Galois theory for q-Galois extensions of simple rings, which is the keynote of the present volume.

Recently, the development of homological algebras enabled us to treat with a kind of Galois theory of general rings. In fact, several results in §9 and outer theory have been extended to more general ring extensions. However, the subject of this volume is restricted to simple ring extensions.

This volume is based on the series of lectures given by one of the authors in 1964-1969 at Hokkaido University, Okayama University and Tsing Hua University. We have tried to make our presentation self-contained. The only knowledge assumed is that of the rudiments of ring and module theory and of topology.

We are greatly indebted to a number of friends for assistance in preparing this manuscript.

1970

H. T.
T. N.

Contents

1. Topological setting

This section contains the preliminary facts on topological spaces, which will be stated without proof. The term topological space is always used to denote one with the T_0-separation axiom.

Let X be a compact space, and Y a topological space. Every closed subset of X is compact. Conversely, if X is a subspace of a Hausdorff space W then X is closed in W. If f is a continuous mapping of X into Y then the image is a compact subset of Y. If f is a continuous 1-1 mappings of X onto a Hausdorff space Y then f is a homeomorphism. Finally, if $\{X_\lambda ; \lambda \in \Lambda\}$ is a collection of compact spaces then the cartesian product $\prod X_\lambda$ is compact.

An <u>inverse system</u> of sets $\{X, \pi\}$ over a directed set Λ is defined as a function which attaches to each $\alpha \in \Lambda$ a set X_α, and to each pair $\alpha \leqslant \beta$ a map π_α^β of X_β into X_α such that $\pi_\alpha^\alpha =$ identity and $\pi_\beta^\gamma \pi_\alpha^\beta = \pi_\alpha^\gamma$ for $\alpha \leqslant \beta \leqslant \gamma$. The maps π_α^β are called <u>projections</u> of the system. If each X_α is a topological space (resp. a topological group) and each projection is continuous (resp. a continuous homomorphism) then $\{X, \pi\}$ is called an inverse system of topological spaces (resp. of topological groups). Let $\{X, \pi\}$ be an inverse system of sets over the directed set Λ. The <u>inverse limit</u> $X_\infty = \varprojlim X_\alpha$ of $\{X, \pi\}$ is defined to be the subset of the cartesian product $\prod X_\alpha$ consisting of those elements $x = (x_\alpha)$ such that $x_\beta \pi_\alpha^\beta = x_\alpha$ for each pair $\alpha \leqslant \beta$. We define then the projection π_α of X_∞ into X_α by $x\pi_\alpha = x_\alpha$. If $\{X, \pi\}$ is an inverse system of topological spaces (resp. of groups) then X_∞ is a toplogical subspace (resp. a subgroup) of $\prod X_\alpha$ and π_α is continuous (resp. a homomorphism). The following is well-known:

Proposition 1.1. Let $\{X, \pi\}$ be an inverse system of non-empty compact Hausdorff spaces.

(a) X_∞ is a non-empty compact Hausdorff space.

(b) If every projection is a mapping onto then so is every π_α.

Finally, we shall glance upon the finite topology. Suppose first that X and Y are arbitrary sets and let Y^X denote the set of all mappings of X into Y. We now introduce the product topology in Y^X considering the space Y as discrete. In this topology, the collection of sets of the form $\{g \in Y^X;\ x_i g = x_i f\}$ where $\{x_i\}$ is a finite subset of X and f is a fixed element of Y^X is a basis for the open sets. From now on we shall refer to the topology we have introduced in Y^X as the finite topology. If X and Y are abelian additive group with an operator domain Ω, then the additive group $\mathrm{Hom}_\Omega(X, Y)$ of Ω-homomorphisms of X into Y is a closed subset of Y^X and a topological group, and $\mathrm{Hom}_\Omega(X, X)$ is a topological ring. At last, suppose that X is a ring and let $\mathcal{G}$ denote the group of all ring automorphisms of X leaving invariant every element of a fixed subset S of X. Then, one will see that $\mathcal{G}$ is a (totally disconnected) topological group in the finite topology.

Bourbaki [3]; Eilenberg-Steenrod [1]; Jacobson [6].

2. A-module

Let A be a ring, and M a right A-module. Often M will be denoted as M_A, and similarly a left A-module M' will be as ${}_AM'$. If $xA \neq 0$ for every non-zero x in M then M is called unital. In case A contains 1, M is unital if and only if $x1 = x$ for every $x \in M$. If $Ma \neq 0$ for every non-zero $a \in A$ then M is called faithful. If $MA \neq 0$ and there is no proper submodule of M other than 0, M is defined to be irreducible. Similarly, a (two-sided) B-A-module M'' is irreducible if $BM''A \neq 0$ and there no proper B-A-submodule of M'' other than 0. A right A-module, or an A-B-module, is called completely reducible if and only if the module is the sum of its irreducible submodules. The following will be familiar:

Proposition 2.1. *Let M be completely reducible: $M = \sum_{\lambda\in\Lambda} M_\lambda$ with irreducible M_λ.*

(a) *$M = \bigoplus_{\lambda\in\Lambda'} M_\lambda$ (direct sum) where Λ' is a suitable subset of Λ, and the cardinal number $\#\Lambda'$ of Λ' is an invariant of M, which will be denoted by $[M|A]$.*

(b) *Every homomorphic image of M is completely reducible, and every submodule of M is a direct summand of M.*

Let M be completely reducible and $M = \bigoplus_{\lambda\in\Lambda} M_\lambda$ with irreducible M_λ. For a fixed τ, we shall denote by M^*_τ the sum of all the M_λ's those which are isomorphic to M_τ. Then, it follows $M = \bigoplus_\tau M^*_\tau$. Now, considering the projection of an arbitrary irreducible submodule N of M into M_λ, we can readily see that N is contained in some M^*_τ. Thus we have seen that each M^*_τ is determined independently on the decomposition $M = \bigoplus_{\lambda\in\Lambda} M_\lambda$. Each M^*_τ is called a homogeneous component of the completely reducible module M, and the unique decomposition $M = \bigoplus_\tau M^*_\tau$ is called the idealistic decomposition of M. In particular, if M is itself a homogeneous component, M is said to be homogeneously completely reducible.

In case an A-module M contains an irreducible submodule, the sum M^* ($\neq 0$) of all the irreducible submodules is called the socle of M. If the right A-module A contains the non-zero socle, every homogeneous component of the socle is an ideal of A.

The following stated without proof will be easily seen:

Proposition 2.2. Let $M = \bigoplus_\tau M^*_\tau$ be the idealistic decomposition of a completely reducible module M_A.

(a) If N is a non-zero submodule of M then non-zero $M^*_\tau \cap N$ exhaust the homogeneous components of N.

(b) The endomorphism ring $E(M_A)$ (acting on the left side) is the complete direct sum of $E(M^*_{\tau A})$.

Proposition 2.3. Let M be a left Q-module and let $A = E({}_QM)$ (acting on the right side).

(a) If e is an idempotent of A then $E({}_QMe)$ is isomorphic to eAe. In case ${}_QM$ is completely reducible, A is isomorphic to the complete direct sum of $e_\tau Ae_\tau$, where e_τ is the projection of M onto its homogeneous component M^*_τ.

(b) If M is homogeneously Q-completely reducible then M is Q-A-irreducible.

The next is the key result for the consideration of completely reducible modules.

Lemma 2.4. Let M_1 and M_2 be left Q-modules. Let A be a ring of Q-endomorphisms of M_2 and B an additive group of Q-homomorphisms of M_1 into M_2 such that $BA \subset B$. Assume that any A-homomorphism of any A-submodule of M_2 into the A-module M_2 can be realized by an element of Q. If $\{ u_i ; i = 1, \dots, n \}$ is an arbitrary finite subset of M_1 then $B^\perp + \sum_1^n Qu_i = (\{u_1, \dots, u_n\}^\perp \cap B)^\perp$, where $(*)^\perp$ means the annihilator of * in the additive group of Q-homomorphisms of M_1 into M_2 or in M_1 according as * is a subset of M_1 or a subset of the additive group of Q-homomorphisms of M_1 into M_2.

Proof. First let $n = 1$ and write u for u_1. It is clear that $B^{\perp} + Qu \subset (u^{\perp} \cap B)^{\perp}$. If $v \in (u^{\perp} \cap B)^{\perp}$ and $b \in u^{\perp} \cap B$, then $vb = 0$. Hence, $ub \longrightarrow vb$ $(b \in B)$ is a single valued mapping of $uB (\subset M_2)$ into M_2. Since $BA \subset B$, uB is an A-submodule of M_2 and our mapping is an A-homomorphism. Hence, there exists an element $q \in Q$ such that $q(ub) = vb$ for all $b \in B$. Thus $(v - qu)B = 0$, which means $v \in B^{\perp} + Qu$. This proves evidently the case $n = 1$. Assume next that $B^{\perp} + \sum_1^{n-1} Qu_j = (\{u_1, \cdots, u_{n-1}\}^{\perp} \cap B)$. Set $B' = \{u_1, \cdots, u_{n-1}\}^{\perp} \cap B$. Then, B' is a subgroup of B and $B'A \subset B'$. Hence, by the case $n = 1$, $B^{\perp} + \sum_1^{n} Qu_j = B'^{\perp} + Qu_n = (u_n^{\perp} \cap B')^{\perp} = (\{u_1, \cdots, u_n\}^{\perp} \cap B)^{\perp}$.

Theorem 2.5. Let M_A be faithful and completely reducible. If $Q = E(M_A)$ and $\mathfrak{L} = E({}_Q M)$, then $\mathfrak{L}$ is the closure of A in the finite topology.

Proof. Consider the Q-submodule $\sum Qx$, where x ranges over all the non-zero elements belonging to irreducible A-submodules of M. Obviously, $\sum Qx$ coincides with M. Each Qx is irreducible as a left Q-module. In fact, for any non-zero qx $(q \in Q)$, the mapping $u \longrightarrow qu$ $(u \in xA)$ is an A-isomorphism of xA into M, which can be extended to an A-automorphism q_o of M (Props. 2.1 and 2.2). Hence, $Qqx = Qq_o q_o^{-1} qx = Qx$. We may set therefore $M = \oplus_{\lambda \in \Lambda} Qx$, where $\{x_\lambda ; \lambda \in \Lambda\}$ is a suitable subset of $\{x\text{'s}\}$. Now, we shall proceed into the proof of our theorem. To our end, it suffices to prove that if α is in $\mathfrak{L}$ and $\{x_1, \cdots, x_n\}$ is a finite subset of $\{x_\lambda\}$ then there exists an $a \in A$ such that $x_i a = x_i \alpha$ $(i = 1, \cdots, n)$. We now apply Lemma 2.4. It should be observed that the hypothesis of our lemma holds good (Prop. 2.1). The conslusion states that there exist $a_j \in A$ $(j = 1, \cdots, n)$ such that $x_i a_j = 0$ for $i \neq j$ and $x_j a_j \neq 0$. We can find moreover

some $e_j \in A$ $(j = 1, \dots, n)$ such that $x_j a_j e_j = x_j \alpha$. In fact, $N = x_j A = x_j a_j A$ is an irreducible direct summand of M_A: $M = N \oplus N'$. If $q' \in Q$ is the projection on N determined by the last decomposition then $x_j \alpha = (q' x_j)\alpha = q'(x_j \alpha) \in N$. Then, $a = \sum_1^n a_j e_j$ is an element requested.

In the rest of this section, otherwise specified, we shall assume always that a ring possesses the identity element 1 and a module is unital, and that a subring is unital, namely, contains 1.

The next is very easy, however, is often of use.

Proposition 2.6. *Let* B *be a subring of* A. *If a left* B-*module* M *possesses a* (*free*) B-*basis* $\{x_1, \dots, x_n\}$ *then the right* A-*module* $\mathrm{Hom}_B(M, A) = \mathrm{Hom}({}_BM, {}_BA)$ *of all* B-*homomorphisms of* M *into* A *possesses an* A-*basis* $\{\alpha_1, \cdots, \alpha_n\}$ *where* α_j *is defined as follows:* $x_i \alpha_j = \delta_{ij}$ $(i, j = 1, \dots, n)$.

A right A-module M is called *projective* if given any homomorphism $\phi: M_A \longrightarrow N'_A$ and any epimorphism $\psi : N_A \longrightarrow N'_A$ there exists a homomorphism $\rho : M_A \longrightarrow N_A$ with $\psi\rho = \phi$ (acting on the left side). The next is familiar, and so the proof may be omitted.

Proposition 2.7. *The direct sum* $M = \bigoplus_{\lambda \in \Lambda} M_\lambda$ *of right* A-*modules* M_λ *is projective if and only if every* M_λ *is projective*.

As an easy consequence of Prop. 2.7, we see that M_A is projective if and only if it is a direct summand of a free A-module.

Proposition 2.8. M_A *is projective if and only if there exist a family* $\{x_\alpha\}$ *of elements of* M *and a family* $\{f_\alpha\}$ *of homomorphisms* $f_\alpha : M_A \longrightarrow A_A$ *such that* $x = \sum_\alpha x_\alpha \cdot f_\alpha x$ *for all* $x \in M$, *where* $f_\alpha x = 0$ *for almost all* α . *In particular,* M_A *is projective and finitely generated if and only if there exist* $\{x_1, \dots, x_n\} \subset M$ *and* $\{f_1, \dots, f_n\} \subset \mathrm{Hom}(M_A, A_A)$ *such that* $x = \sum_i x_i \cdot f_i x$ *for all* $x \in M$.

Proof. Let $\phi : F_A \longrightarrow M_A$ be an epimorphism of a free A-module F with a basis $\{e_\alpha\}$ onto M, and let $x_\alpha = \phi e_\alpha$. In order

that M_A be projective it is necessary and sufficient that there exist a homomorphism $f: M_A \longrightarrow F_A$ such that $\phi f = 1$. If we write $fx = \sum_\alpha e_\alpha \cdot f_\alpha x$, we obtain homomorphisms $f_\alpha : M_A \longrightarrow A_A$ such that for each $x \in M$ there holds $f_\alpha x = 0$ for almost all α. The condition $\phi f = 1$ is then equivalent with $x = \sum_\alpha x_\alpha \cdot f_\alpha x$ for all $x \in M$.

For an arbitrary M_A we set $t(M_A) = \sum fM$ where f ranges over all the homomorphisms of M_A into A_A. Then, $t(M_A)$ is a two-sided ideal of A and called the trace ideal of M_A. Similarly, the trace ideal of a left A-module can be defined. If $t(M_A) = A$, namely, if there exist a family $\{ x_1, \dots, x_n \}$ $(x_i \in M)$ and a family $\{ f_1, \dots, f_n \}$ of A-homomorphisms of M_A into A_A such that $\sum_1^n f_i x_i = 1$, then M_A is called completely faithful. Assume now that M_A be completely faithful: $\sum_1^n f_i x_i = 1$. Then, $(y_1, \dots, y_n) \longrightarrow \sum_1^n f_i y_i$ defines an epimorphism $\phi : M_A^{(n)} \longrightarrow A_A$, where $M_A^{(n)}$ means the direct sum of n copies of M_A. (Similarly, in case M is a left A-module, the direct sum of n copies of ${}_AM$ will be denoted by ${}_A^{(n)}M$.) Conversely, assume that ϕ is an epimorphism of $M_A^{(n)}$ onto A_A. We define here the homomorphism $g_i : M_A \longrightarrow M_A^{(n)}$ by $g_i y = (0, \dots, \overset{i}{\underset{\smile}{y}}, \dots 0)$. Then $f_i = \phi g_i : M_A \longrightarrow A_A$ and $\phi(y_1, \dots, y_n) = \phi(\sum_1^n g_i y_i) = \sum_1^n f_i y_i$. Recalling that ϕ is an epimorphism, we can find a family $\{ x_1, \dots, x_n \}$ $(x_i \in M)$ with $\sum_1^n f_i x_i = 1$. We have proved thus the following:

Proposition 2.9. In order that M_A be completely faithful it is necessary and sufficient that there exist a positive integer n such that A_A is a homomorphic image (or isomorphic to an A-direct summand) of $M_A^{(n)}$. In particular, if M_A is completely faithful then it is faithful.

If there exist positive integers r, s such that $M_A^{(r)}$ is isomorphic to $A_A^{(s)}$, M_A is said to be regular. If every irreducible right A-module is a homomorphic image of M_A, M_A is said to be upper distinguished. Obviously, A_A is upper distinguished.

Proposition 2.10. (a) *If M_A is regular then M_A is finitely generated and completely faithful.*

(b) *If M_A is completely faithful then M_A is upper distinguished.*

(c) *If M_A is projective and upper distinguished then M_A is completely faithful.*

Proof. (a) is clear by Prop. 2.9. We assume now that M_A is completely faithful. If $\mathfrak{N}$ is an arbitrary maximal right ideal of A, we can find a homomorphism $f: M_A \longrightarrow A_A$ such that $fM \not\subset \mathfrak{N}$, and then $x \longrightarrow fx + \mathfrak{N}$ defines an epimorphism of M_A onto the irreducible A-module $A/\mathfrak{N}$, which proves (b). Finally, we shall prove (c). Suppose on the contrary $t(M_A) \neq A$, and choose a maximal right ideal $\mathfrak{N}$ of A containing $t(M_A)$. By assumption, we can find then an epimorphism $g: M_A \longrightarrow A/\mathfrak{N}$. If ν is the natural homomorphism of A onto $A/\mathfrak{N}$, M_A being projective, there exists a homomorphism $f: M_A \longrightarrow A_A$ with $\nu f = g$, whence it follows $\nu(fM) = gM = A/\mathfrak{N}$. We obtain thus $fM \not\subset \mathfrak{N}$, which contradicts $t(M_A) \subset \mathfrak{N}$.

Corollary 2.11. *Let A be a commutative ring. If M_A is finitely generated, projective and faithful then it is completely faithful.*

Proof. We shall prove first that if M_A is finitely generated and faithful then M_A is upper distinguished. Let $M = \sum_1^n u_i A$ be faithful. If $\mathfrak{m}$ is an arbitrary maximal ideal of A then $M\mathfrak{m} \neq M$. For, if not, we have $\sum_1^n u_i \mathfrak{m} = M$, and then there exists a family $\{a_{ij};\ i, j = 1, \ldots, n\}$ $(a_{ij} \in \mathfrak{m})$ such that $\sum_1^n u_i(\delta_{ij} - a_{ij}) = 0$ $(j = 1, \ldots, n)$. Then, we readily obtain $M \cdot \det(\delta_{ij} - a_{ij}) = 0$, whence it follows $\det(\delta_{ij} - a_{ij}) = 0$.

On the other hand, there holds $\det(\delta_{ij} - a_{ij}) \equiv 1 \bmod \mathfrak{m}$, and we have a contradiction $1 \in \mathfrak{m}$. Since $M/M\mathfrak{m}$ can be regarded as a non-zero module over the field $A/\mathfrak{m}$, $A/\mathfrak{m}$ is a homomorphic image (of $M/M\mathfrak{m}$ and so) of M_A. Now, the corollary is a consequence of Prop. 2.10 (c).

Proposition 2.12. *Let* B *be a subring of* A. *If* A_B *is completely faithful then* B *is a direct summand of* A_B, *and conversely*.

Proof. The converse part is contained in Prop. 2.9. Suppose that A_B is completely faithful: $\sum_1^n f_i a_i = 1$ ($a_i \in A$, $f_i \in \mathrm{Hom}(A_B, B_B)$). Then, $x \longrightarrow \sum_1^n f_i(a_i x)$ defines a homomorphism $f: A_B \longrightarrow B_B$. Since $f(1) = \sum_1^n f_i a_i = 1$, we see that $f(b) = b$ for every $b \in B$. Hence, we obtain at once $A = B \oplus \mathrm{Ker}\, f$.

Now, we shall prove the following:

Theorem 2.13. *Let* $Q = E(M_A)$ (*acting on the left side*).

(a) *If* M_A *is completely faithful then* ${}_Q M$ *is finitely generated and projective and* A *coincides with* $E({}_Q M)$.

(b) *If* M_A *is fainitely generated and projective then* ${}_Q M$ *is completely faithful*.

Proof. (a) Let f be an arbitrary element of $\mathrm{Hom}(M_A, A_A)$. For each $y \in M$, $x \longrightarrow y \cdot fx$ defines an element $q_y \in Q$: $y \cdot fx = q_y x$. To be easily verified, the mapping $y \longrightarrow q_y$ is a homomorphism $g: {}_Q M \longrightarrow {}_Q Q$ and we have $y \cdot fx = yg \cdot x$ for all $x, y \in M$. Now, assume that M_A is completely faithful: $\sum_1^n f_i x_i = 1$ ($x_i \in M$, $f_i \in \mathrm{Hom}(M_A, A_A)$). Then, by the above argument, we can find homomorphisms $g_i: {}_Q M \longrightarrow {}_Q Q$ with $y \cdot f_i x = y g_i \cdot x$ for all $x, y \in M$. Accordingly, there holds $\sum_1^n y g_i \cdot x_i = \sum_1^n y \cdot f_i x_i = y$ for all $y \in M$, which proves that ${}_Q M$ is finitely generated and projective (Prop. 2.8). Next, take an arbitrary element $\alpha \in E({}_Q M)$, and set $a = \sum_1^n f_i(x_i \alpha)$. Then, for each $y \in M$ we have $ya = \sum_1^n y \cdot f_i(x_i \alpha) = \sum_1^n y g_i \cdot x_i \alpha = (\sum_1^n y g_i \cdot x_i)\alpha = y\alpha$, which implies $\alpha = a \in A$.

(b) Assume that M_A is finitely generated and projective: $\sum_1^n x_i \cdot f_i x = x$ for all $x \in M$ with some $x_i \in M$ and $f_i \in \mathrm{Hom}(M_A, A_A)$ (Prop. 2.8). As in the proof of (a), we can find then the homomorphisms $g_i : {}_QM \longrightarrow {}_QQ$ with $y \cdot f_i x = y g_i \cdot x$ for all x, y in M. Accordingly, we see that $x = \sum_1^n x_i \cdot f_i x = \sum_1^n x_i g_i \cdot x$ for all $x \in M$, which implies that $\sum_1^n x_i g_i = 1$. We have proved thus ${}_QM$ is completely faithful.

If M is a Q-A-module then $M^{(r)}$ and ${}^{(s)}M$ may be regarded naturally as a $(Q)_r$-A-module and as a Q-$(A)_s$-module, respectively. Under this situation, we obtain the following, whose proof may be left to readers.

Lemma 2.14. (a) $A = E({}_QM)$ *if and only if* $A = E({}_{(Q)_r}M^{(r)})$.

(b) $Q = E(M_A)$ *if and only if* $(Q)_r = E(M_A^{(r)})$.

Theorem 2.15. *If* (M_A *is regular and*) $M_A^{(r)} \simeq A_A^{(s)}$ *and* $Q = E(M_A)$ *then* $A = E({}_QM)$ (*or what is the same,* A *coincides with the double centralizer* $V_{\mathfrak{ol}}^2(A)$ *of* A *in the absolute endomorphism ring of* M), ${}^{(s)}_QM \simeq {}^{(r)}_QQ$ *and* $(Q)_r \simeq (A)_s$.

Proof. The first assertion is a consequence of Prop. 2.10 (a) and Th. 2.13 (a). The $(Q)_r$-$(A)_s$-module $\mathfrak{M} = {}^{(s)}(M^{(r)}) = ({}^{(s)}M)^{(r)}$ is nothing but the module consisting of all $r \times s$ matrices with entries in M. As $Q = E({}^{(s)}M_{(A)_s})$ (cf. Lemma 2.14 (a)), we have $(Q)_r = E(\mathfrak{M}_{(A)_s})$ by Lemma 2.14 (b). To be easily verified, $M_A^{(r)} \simeq A_A^{(s)}$ is equivalent with the condition that $\mathfrak{M} = \mathfrak{m}(A)_s$ with some $(A)_s$-free element $\mathfrak{m} \in \mathfrak{M}$. Accordingly, for each $X \in (A)_s$ there exists a uniquely determined $Y \in E(\mathfrak{M}_{(A)_s}) = (Q)_r$ such that $Y\mathfrak{m} = \mathfrak{m}X$, which proves that $\mathfrak{m}$ is $(Q)_r$-free and $\mathfrak{M} = (Q)_r\mathfrak{m}$. Hence, we have ${}^{(s)}_QM \simeq {}^{(r)}_QQ$. Moreover, we can easily see that $X \longrightarrow Y$ defines a ring isomorphism between $(A)_s$ and $(Q)_r$.

Azumaya [3], [4]; Azumaya-Nakayama [2]; Cartan-Eilenberg [1]; Jacobson [1], [6].

3. Simple ring

A ring A is called (right) primitive if there exists a faithful irreducible right A-module. Now, let M_A be a faithful irreducible right A-module, and $D = E(M_A)$. Then, A is dense in the linear transformation ring $\mathfrak{L} = E({}_DM)$ (Th. 2.5).

Proposition 3.1. If A is a primitive ring then there exists a division ring D such that A is isomorphic to the complete matrix ring $(D)_n$ over D or for each positive integer m there exists a homomorphism of a subring of A onto $(D)_m$. In particular, if the primitive ring is right Artinian (i.e. if A satisfies the minimum condition for right ideals) then A is isomorphic to $(D)_n$.

Proof. Regarding A as a dense subring of the linear transformation ring $\mathfrak{L}$ of a left vector space M over a division ring D, the two conclusions correspond to the following possibilities: (i) M is n dimensional over D: $[M:D]_L = n < \infty$ and (ii) $[M:D]_L = \infty$. In the case (i) we have seen $A = \mathfrak{L} \simeq (D)_n$. While, in the case (ii), M has a subspace N with $[N:D]_L = m$. Then, $T = \{ a \in A;\ Na \subset N \}$ is evidently a subring of A and the contraction map $a \longrightarrow N|a$ $(a \in T)$ gives an epimorphism onto $E({}_DN) \simeq (D)_m$. If A is right Artinian then M is finite dimensional over D. Otherwise, we can find a denumerable infinite set $\{ u_1, u_2, \dots \}$ of linearly independent elements in M. Then by the density of A there holds $u_1^{\perp} \cap A \supsetneqq \{u_1, u_2\}^{\perp} \cap A \supsetneqq \{ u_1, u_2, u_3 \}^{\perp} \cap A \supsetneqq \dots$, which is a contradiction.

A ring A is called two-sided simple if A contains no proper ideals except 0, and a right Artinian two-sided simple ring with 1 is called a simple ring. If A is a simple ring then A_A coincides with its socle and homogeneously completely reducible. It follows therefore A is a direct sum of a finite number of isomphic minimal right ideals: $A = \mathfrak{r}_1 \oplus \dots \oplus \mathfrak{r}_n$ and $n = [A_A|\, A]$. Since every minimal right ideal $\mathfrak{r}$ of A is an irreducible, faithful (more precisely completely faithful) right A-module, A is primitive. Further, A is the complete $n \times n$ matrix ring over a division ring D (Th. 2.15).

The following lemma will be familiar.

Lemma 3.2. *Assume a ring* $A \ni 1$ *contains a system of matrix units* $\{c_{ij}\}$, *and let* $A_o = V_A(\{c_{ij}\})$ (*the centralizer of* $\{c_{ij}\}$ *in* A).

(a) A *is the complete matrix ring over* A_o: $A = \sum A_o c_{ij}$.

(b) A *is right Artinian* (*resp. Noetherian*) *if and only if so is* A_o.

(c) A *is two-sided simple if and only if so is* A_o.

Combining Prop. 3.1 with the above lemma, one will readily obtain the following:

Theorem 3.3. *A simple ring may be defined as a left Artinian two-sided simple ring with* 1. *A ring* A *is simple if and only if* A *is isomorphic to the complete* $n \times n$ *matrix ring over a division ring* D, *where* $n = |A|$ *is an invariant of* A *and* D *is unique up to isomorphisms*.

Let A be a simple ring. If $A = \sum_1^n De_{ij}$ with a system of matrix units $\{e_{ij}\}$ and a division ring $D = V_A(\{e_{ij}\})$, n and D are called the *capacity* of A and *a division ring belonging to* A, respectively. To be easily seen, every unital A-module is completely faithful and homogeneously completely reducible, and there exists essentially only one irreducible A-module.

Proposition 3.4. *Let* A *be a simple ring. If* M *is a unital* A-A-*module then* M *possesses a right* (*resp. left*) A-*basis*.

Proof. If $A = \sum_{i,j=1}^n De_{ij}$ with a system of matrix units $\{e_{ij}$'s$\}$ and a division ring $D = V_A(\{e_{ij}$'s$\})$, then $M = e_{11}M \oplus \dots \oplus e_{nn}M$. Since $e_{ii}M_A \simeq e_{1i}e_{ii}M_A \simeq e_{11}M_A \simeq e_{11}A_A^{(\lambda)}$ with some cardinal number λ, we readily obtain $M_A \simeq e_{11}A_A^{(n\lambda)} \simeq A_A^{(\lambda)}$.

If M is in addition a unital left A-module that possesses a left A-basis, and the right dimension coincides with the left one, we denote those equal dimensions by $[M:A]$.

Proposition 3.5. Every element of a simple ring A is a finite sum of units.

Proof. We set again $A = \sum_1^n De_{ij}$ with a system of matrix units $\{e_{ij}\}$ and the division ring $D = V_A(\{e_{ij}\})$. To our end, it suffices to consider the case $n > 1$. For $i \neq j$, there holds $(1 - e_{ij})(1 + e_{ij}) = 1$. Hence, $a_{ij} = 1 - e_{ij}$ $(i \neq j)$, $a_{ii} = a_{il}a_{li}$ $(i \neq 1)$ and $a_{11} = 1$ are units. One can easily see that every e_{ij} is represented by those a_{ij}'s.

Let S be a unital subring of R. R is said to be left (resp. right) k-algebraic over S if $S[x_1, \ldots, x_k]$ is left finite (resp. right finite) over S for every $x_1, \ldots, x_k$ in R. In particular, if R is left (resp. right) 1-algebraic over S, following Jacobson, R is called left (resp. right) algebraic over S. If R is left (resp. right) k-algebraic over S for every positive integer k, or, if $S[F]$ is left finite (resp. right finite) over S for every finite subset F of R, then R is defined to be left (resp. right) locally finite over S. If R is left algebraic over a unital simple subring A and r is a unit of R then r^{-1} is contained in $A[r]$. In what follows, the remark will be used often without mention.

Proposition 3.6. Let A be a unital simple subring of a simple ring R.

(a) $|A|$ is a divisor of $|R|$ and R possesses an A-basis consisting of units.

(b) If $|R| = |A|$ then for each $x \in R$ and for each simple intermediate ring T of R/A there holds $[xA|A] \geqslant [xT|T]$. If moreover R/A is left locally finite and $[T:A]_L < \infty$ then there exists an intermediate ring T' of R/T such that $[T':A]_L < \infty$ and $[xT'|T'] = [xR|R]$.

Proof. Let $A = \sum_1^n De_{ij}$ with a system of matrix units $\{e_{ij}\}$ and the division ring $D = V_A(\{e_{ij}\})$. Then $R = e_{11}R \oplus \ldots \oplus e_{nn}R$

and $R_o = V_R(\{e_{ij}\})$ is simple (Lemma 3.2). Since $e_{ii}R$ is isomorphic to $e_{jj}R$ by the left multilication of e_{ji}, (a) is clear by Prop. 3.5. The remainder will be almost evident.

Proposition 3.7. Let A be a simple ring. If $\{A_\lambda ; \lambda \in \Lambda\}$ is a directed set (with respect to inclusion) of unital simple subrings A_λ of A then $T = \bigcup_\lambda A_\lambda$ is a simple ring.

Proof. Let $A_o = \sum D_o f_{ij}$ be a member of $\{A_\lambda\}$ of the greatest capacity ($\leqslant |A|$), where $\{f_{ij}\}$ is a system of matrix units with the division ring $D_o = V_{A_o}(\{f_{ij}\})$. Then every A_λ containing A_o is represented as $\sum D_\lambda f_{ij}$ with the division ring $D_\lambda = V_{A_\lambda}(\{f_{ij}\})$. The simplicity of T is therefore evident.

Proposition 3.8. (a) Let B be a left Artinian unital subring of $R \ni 1$. If A is an intermediate ring of R/B left finite over B such that R is A-R-irreducible, then A is a simple ring. In particular, if R is two-sided simple and coincides with $B \cdot V_R(R)$ then B is a simple ring.

(b) Let B be a unital simple subring of a simple ring R, and let R be left locally finite over B. If R is B-R-irreducible then every intermediate ring of R/B is simple.

Proof. (a) Obviously, A is left Artinian. Then there exists a minimal left ideal $\mathfrak{k}$ of A and there holds $R = A\mathfrak{k}R = \sum_{x \in R} \mathfrak{k}x$, which means that R is homogeneously completely reducible as left A-module. Hence, A is so. It follows therefore that A is a simple ring (Lemma 2.14).

(b) If A is an arbitrary intermediate ring of R/B then $A = \bigcup_\lambda A_\lambda$ where A_λ runs over all the intermediate rings of A/B left finite over B. Since R is evidently A_λ-R-irreducible, each A_λ is simple by (a). Now, our assertion is a consequence of Prop. 3.7.

For a ring A with 1, A^* will denote the multiplicative group of all the units of A.

Lemma 3.9. Let A be an infinite simple ring, and B a unital subring of A. If the group index $(A^{\cdot}:B^{\cdot})$ is finite then $A = B$.

Proof. If a is an arbitrary element of $A^{\cdot} \cap B$ then there exists a positive integer m with $a^m \in B^{\cdot}$, whence we see that a has to be contained in $B^{\cdot}$. Hence, we have $B^{\cdot} = A^{\cdot} \cap B$. Now, we set $A = \sum_1^n De_{ij}$ with a system of matrix units $\{e_{ij}\}$ and the division ring $D = V_A(\{e_{ij}\})$, and distinguish between two cases.

Case I. $n = 1$: As was noted just above, there holds $B^{\cdot} = D^{\cdot} \cap B = B\backslash\{0\}$ (the completment of $\{0\}$ in B), which proves that B is a division ring. If $[A:B]_L > 1$ on the contrary, we can find an element $a \in A\backslash B$. Since $\{1, a\}$ is left B-free, for each different b_1, b_2 in B, $1 + b_1a$ and $1 + b_2a$ are contained in $A^{\cdot}$ and not congruent modulo $B^{\cdot}$. It follows therefore a contradiction $(A^{\cdot}:B^{\cdot}) \geqslant \# B^{\cdot} = \# A^{\cdot}$.

Case II. $n > 1$: Evidently, D is infinite and $(D^{\cdot}:(D \cap B)^{\cdot})$ is finite. Accordingly, by the first case, $D = D \cap B$, or what is the same $D \subset B$. Now, for each $i \neq j$ and $d \in D^{\cdot}$, $d + e_{ij}$ is in $A^{\cdot}$ and we see that $\#\{d + e_{ij};\ d \in D^{\cdot}\} = \# D$. Thus, there exist some b in $B^{\cdot}$ and $d_1 \neq d_2$ in $D^{\cdot}$ such that $d_1 + e_{ij} = b(d_2 + e_{ij})$, which means $b = (d_1 + e_{ij})(d_2 + e_{ij})^{-1} = d_1d_2^{-1} + (1 - d_1d_2^{-1})d_2^{-1}e_{ij}$. Recalling here that $d_1 \neq d_2$ and $D \subset B$, it follows at once $e_{ij} \in B$ for each $i \neq j$. From this, it will be easy to see that all e_{ij}'s are contained in B. Consequently, $A = B$.

Proposition 3.10. Let $T \ni 1$ be a ring, and A a unital simple subring of T. If $\#\{ata^{-1};\ a \in A^{\cdot}\} < \infty$ for every $t \in T$ then either $\# A < \infty$ or $A \subset V_T(T)$.

Proof. If A is infinite then $(A^{\cdot}:V_A(t)^{\cdot}) = \#\{ata^{-1};\ a \in A^{\cdot}\} < \infty$ yields $A = V_A(t)$ (Lemma 3.9), whence it follows $A = V_A(T) \subset V_T(T)$.

The next theorem is fundamental in the study of simple rings.

Theorem 3.11. Let B be a unital simple subring of a simple ring A with $[A:B]_R < \infty$, and M a unital finitely generated right A-module. (One may regard A as a subring of $\mathcal{O}\!\!\mathcal{L} = \mathrm{Hom}(M, M)$.)

(a) $V_{\mathcal{O}\!\!\mathcal{L}}(B)$ is a simple ring, $V^2_{\mathcal{O}\!\!\mathcal{L}}(B) = B$ and $[A:B]_R = [V_{\mathcal{O}\!\!\mathcal{L}}(B):V_{\mathcal{O}\!\!\mathcal{L}}(A)]_R$.

(b) If ϕ is an isomorphism of A onto an intermediate ring A' of $\mathcal{O}\!\!\mathcal{L}/B$ and $B\phi = B$, then ϕ can be extended to an inner automorphism of $\mathcal{O}\!\!\mathcal{L}$.

Proof. (a) As M_A is regular: $M_A^{(r)} \simeq A_A^{(s)}$, $[A:B]_R = p$ yields $M_B^{(r)} \simeq B_B^{(ps)}$. We set $Q = E(M_A)$ and $P = E(M_B)$, which are anti-isomorphic to $V_{\mathcal{O}\!\!\mathcal{L}}(A)$ and $V_{\mathcal{O}\!\!\mathcal{L}}(B)$, respectively. By Th. 2.15, $V^2_{\mathcal{O}\!\!\mathcal{L}}(B) = B$ and $(P)_r \simeq (B)_{ps}$. Since $(B)_{ps}$ is simple, so is $V_{\mathcal{O}\!\!\mathcal{L}}(B)$ by Lemma 3.2. In particular, $V_{\mathcal{O}\!\!\mathcal{L}}(A)$ is simple. Moreover, again by Th. 2.15, we obtain ${}^{(s)}_{Q}M \simeq {}^{(r)}_{Q}Q$ and ${}^{(ps)}_{P}M \simeq {}^{(r)}_{P}P$, whence it follows ${}^{(r)}_{Q}({}^{(p)}_{Q}Q) \simeq {}^{(pr)}_{Q}Q \simeq {}^{(r)}_{Q}P$. Now, Krull-Schmidt theorem yields at once ${}^{(p)}_{Q}Q \simeq {}_{Q}P$, and $[V_{\mathcal{O}\!\!\mathcal{L}}(B):V_{\mathcal{O}\!\!\mathcal{L}}(A)]_R = [P:Q]_L = p = [A:B]_R$.

(b) If $\mathfrak{r}$ is an (essentially unique) minimal right ideal of A then $\mathfrak{r}' = \mathfrak{r}\phi$ is a minimal right ideal of A' and $[\mathfrak{r}'|B] = [\mathfrak{r}|B] (< \infty)$. Since $[M|A]\cdot[\mathfrak{r}|B] = [M|B] = [M|A']\cdot[\mathfrak{r}'|B]$, we obtain $[M|A] = [M|A']$. Hence, there exists an invertible element θ in $\mathcal{O}\!\!\mathcal{L}$ such that $(ua)\theta = (u\theta)\cdot a\phi$ for every $u \in M$ and $a \in A$, which means $a\phi = \theta^{-1}a\theta$.

Given a subset S of a ring A with 1, S_L (resp. S_R) denotes the set of all the left multiplications a_L (resp. the right multolications a_R) in A effected by $a \in S$, and $\tilde{S}$ or $S\tilde{}$ denotes the set of all the inner automorphisms $\tilde{a} = a_L a_R^{-1}$ induced by units a of A contained in S. Writing $M = A$, $A = A_L$ and $B = B_L$ in Th. 3.11, we obtain the next at once:

Corollary 3.12. Let B be a unital simple subring of a simple ring A, and $[A:B]_L < \infty$.

(a) If $\mathfrak{A} = \mathrm{Hom}(A, A)$ then $V_{\mathfrak{A}}(B_L)$ is simple, $V^2_{\mathfrak{A}}(B_L) = B_L$ and $[A:B]_L = [V_{\mathfrak{A}}(B_L):A_R]_R$.

(b) If ϕ is an automorphism of A with $B\phi = B$ then there exists an invertible A_L-semilinear transformation θ whose automorphism is ϕ (regarded as an automorphism of A_L).

If $a_1, \cdots, a_m$ are elements of a ring A then we define $I[a_1, \cdots, a_m] = \sum \pm a_{i_1} a_{i_2} \cdots a_{i_m}$ where the sum is taken over all the permutations of $1, 2, \cdots, m$ and the sign is + or - according as the permutation is even or odd. The identity of the form $I[x_1, \cdots, x_m] = 0$ for a ring A is called the standard identity of degree m for A. It is easy to see that A is an algebra of finite rank m then A satisfies the standard identity of degree $m + 1$. Now, for a field K and a positive integer m, we define $r(K, m)$ to be the minimal degree of the standard identity satisfied by $(K)_m$. Obviously, $r(K, 1) = 2$.

Proposition 3.13. $r(K, m + 1) > r(K, m) + 1$.

Proof. Let $\{e_{ij}\}$ be the system of matrix units of $(K)_m$, and let $a_1, a_2, \cdots, a_{r-1}$ $(r = r(K, m))$ be elements of $(K)_m$ such that $I[a_1, a_2, \cdots, a_{r-1}]$ is non-zero. We assume here that the (p, q)-entry of $I[a_1, a_2, \cdots, a_{r-1}]$ is non-zero. Let $a'_1, a'_2, \cdots, a'_{r-1}$ be respectively the matrices obtained from $a_1, a_2, \cdots, a_{r-1}$ by bordering by the last row and the last column of zeros. Then, one will see that $I[a'_1, \cdots, a'_{r-1}, e_{qm+1}, e_{m+1m+1}] = I[a'_1, \cdots, a'_{r-1}]e_{qm+1} \neq 0$, and that $r(K, m + 1) > r + 1$.

For the sake of the later use, we shall glance here upon the radical of a ring. Every nilpotent one-sided ideal is contained in some nilpotent ideal, and every finite sum of nilpotent ideals is also nilpotent. Hence, we see that the join $\mathfrak{N}$ of all the nilpotent ideals of A is a nil-ideal. If A is right Artinian, then it is well known that every non-nilpotent right ideal of A contains a non-zero idempotent, so that we see that $\mathfrak{N}$ is nilpotent. For a

right (or left) Artinian ring A, the unique maximal nilpotent ideal is called the radical of A, and the radical $\mathfrak{n}(A/\mathfrak{n})$ of $A/\mathfrak{n}$ is zero. As is well known, if A is a right Artinian ring with 1 then the following conditions are equivalent: (1) The radical of A is zero, (2) A_A is completely reducible, and (3) A is a direct sum of simple rings. If a right Artinian ring A with 1 satisfies any of the above equivalent conditions, A is called semi-simple. One will readily see that the notion of semi-simple is right-left symmetric, and that any right Artinian ring with 1 is right Noetherian.

Let e_1 and e_2 be idempotents in a ring A. As is well known, $e_1A \simeq e_2A$ (as right A-module) if and only if there exist $e_{12} \in e_1Ae_2$ and $e_{21} \in e_2Ae_1$ such that $e_{12}e_{21} = e_1$ and $e_{21}e_{12} = e_2$. By the aid of this fact, we can prove the following stated without proof.:

Proposition 3.14. *Let A be a right Artinian ring with 1, $\mathfrak{n}$ its radical, $\bar{A} = A/\mathfrak{n}$, and $\bar{a} = a + \mathfrak{n}$ $(a \in A)$.*

(a) *Let e_1, e_2 be idempotents in A. If $\bar{e}_1\bar{A} \simeq \bar{e}_2\bar{A}$ then $e_1A \simeq e_2A$.*

(b) *If e is a primitive idempotent of A then $e\mathfrak{n} = eA \cap \mathfrak{n}$ is the unique maximal sub-right ideal of eA.*

Let A be a right Artinian ring with 1, $\mathfrak{n}$ its radical, $\bar{A} = A/\mathfrak{n}$ and $\bar{a} = a + \mathfrak{n}$ $(a \in A)$. If we set $A \simeq \oplus_1^m (e_iA)^{(f_i)}$ $(f_i > 0)$ with primitive idempotents $e_1, \cdots, e_m$ such that e_iA and e_jA are not isomorphic provided $i \neq j$, then $\bar{A} \simeq \oplus_1^m (\bar{e}_i\bar{A})^{(f_i)}$ and every $\bar{e}_i\bar{A}$ is irreducible (Prop. 3.14 (b)). Accordingly, every irreducible right $\bar{A}$-module is isomorphic to some $\bar{e}_i\bar{A}$. Now, we shall prove the following:

Proposition 3.15. *Let A be a right Artinian ring with 1, and $A \simeq \oplus_1^m (e_iA)^{(f_i)}$ $(f_i > 0)$ with primitive idempotents $e_1, \cdots, e_m$*

such that e_iA and e_jA are not isomorphic provided $i \neq j$.

(a) If $\oplus_1^m (e_iA)^{(\omega_i)} \simeq \oplus_1^m (e_iA)^{(\omega_i')}$ then $\omega_i = \omega_i'$, where ω_i and ω_i' are (finite or infinite) cardinal numbers.

(b) If M_A is projective then $M_A \simeq \oplus_1^m (e_iA)^{(\omega_i)}$ with some (finite or infinite) cardinal numbers ω_i.

Proof. Let $\mathfrak{n}$ be the radical of A, $\bar{A} = A/\mathfrak{n}$, and $\bar{a} = a + \mathfrak{n}$ $(a \in A)$. (a) is an easy consequence of Props. 2.1 and 3.14. We shall prove now (b). Let $M/M\mathfrak{n} \simeq \oplus_1^m (\bar{e}_i\bar{A})^{(\omega_i)}$. If we set $M_o = \oplus_1^m (e_iA)^{(\omega_i)}$ then there exists an isomorphism $\psi : M_o/M_o\mathfrak{n} \simeq M/M\mathfrak{n}$. Since M_o is projective (Prop. 2.7), for the natural homomorphism $\phi : M \longrightarrow M/M\mathfrak{n}$ and $\phi_o : M_o \longrightarrow M_o/M_o\mathfrak{n}$ there exists a homomorphism $\rho : M_o \longrightarrow M$ such that $\phi\rho = \psi\phi_o$, and so we have $M = \rho M_o + M\mathfrak{n}$. Recalling that $\mathfrak{n}$ is nilpotent, it will be easy to see that $M = \rho M_o$. Since M is projective, we have then $M_o = M' \oplus \operatorname{Ker}\rho = M' + M_o\mathfrak{n}$, whence we obtain our assertion $\operatorname{Ker}\rho = 0$.

The next will play an important role in § 9.

Corollary 3.16. Let A be a right Artinian ring with 1, and let N and P be unital right A-modules.

(a) If P is projective and $P^{(p)} \sim N^{(n)}$ with positive integers $p \leqslant n$ then $P \sim N$.

(b) If $N^{(n)} \simeq A^{(\omega)}$ with a positive integer n and an infinite cardinal number ω then $N \simeq A^{(\omega)}$.

(c) If $N^{(n)} \simeq A^{(a)}$ with positive integers n, a, and $a = nq + r$ $(0 \leqslant r < n)$, then $N \simeq A^{(q)} \oplus N_o$ for a homomorphic image N_o of A such that $N_o^{(n)} \simeq A^{(r)}$.

Proof. As to notations, we follow Prop. 3.15.

(a) Let $N/N\mathfrak{n} \simeq \oplus_1^m (\bar{e}_i\bar{A})^{(\omega_i)}$ and $P \simeq \oplus_1^m (e_iA)^{(\omega_i')}$ (Prop. 3.15). The homomorphism $P^{(p)} \sim N^{(n)}$ induces a homomorphism $P^{(p)}/P^{(p)}\mathfrak{n} \sim N^{(n)}/N^{(n)}\mathfrak{n}$, and so we have $\oplus_1^m (\bar{e}_i\bar{A})^{(p\omega_i')} \sim$

$\oplus_1^m (\bar{e}_i\bar{A})^{(n\omega_i)}$. Since every $\bar{e}_i\bar{A}$ is irreducible (Prop. 3.14) and $p \leqslant n$, we readily see that $\omega_i' \geqslant \omega_i$ $(i = 1, \ldots, m)$, and hence we can find an epimorphism $\pi : P \longrightarrow N/N\mathfrak{n}$. Then, P being projective, for the natural homomrphism $\phi : N \longrightarrow N/N\mathfrak{n}$ we can find a homomorphism $\rho : P \longrightarrow N$ such that $\phi\rho = \pi$. Hence, $N = P\rho + N\mathfrak{n} = P\rho$, for $\mathfrak{n}$ is nilpotent.

(b) and (c) Since the projective module N is isomorphic to $\oplus_1^m (e_iA)^{(\omega_i)}$ (Prop. 3.15 (b)), (b) is an easy consequence of Prop. 3.15 (a). Next, we shall prove (c). Since $\oplus_1^m (e_iA)^{(n\,\omega_i)} \simeq \oplus_1^m (e_iA)^{(af_i)}$, Prop. 3.15 (a) yields $n\,\omega_i = af_i = nqf_i + rf_i$, whence it follows $rf_i = nk_i$ with some k_i $(0 \leqslant k_i < f_i)$. We get therefore $\omega_i = qf_i + k_i$, and so $N_o = \oplus_1^m (e_iA)^{(k_i)}$ satisfies the relation proposed.

Albert [1]; Artin-Whaples [1]; Artin-Nesbitt-Thrall [1]; Azumaya [1], [3]; Azumaya-Nakayama [2]; Jacobson [1], [6]; Kasch [8]; Scott [1]; Tominaga [4], [5].

4. Tensor product of algebras

We suppose the readers are familiar with the elementary results on tensor products of modules and algebras. For the sake of simplicity, in this section we assume always K means a field, a ring contains 1 and a subring is unital. Accordingly, in the tensor product over K of K-algebras A_1, A_2, each A_i may be regarded as a subalgebra of the tensor product. A two-sided simple algebra A over K is said to be central if the center of A coincides with K, and a simple algebra A of finite rank over K is called a separable simple algebra if the center C of A is separable over K. At first, we shall state the following well-known lemma without proof.

Lemma 4.1. *Let A be an algebra over K, and B central two-sided simple algebra over K. The correspondences* $\mathfrak{M} \longrightarrow \mathfrak{M} \cap A$ *and* $\mathfrak{m} \longrightarrow \mathfrak{m} \otimes_K B$ *are mutually converse 1-1 correspondences between B-B-submodules* $\mathfrak{M}$ *of* $A \otimes_K B$ *and K-submodules* $\mathfrak{m}$ *of A. The same induce also 1-1 correspondences between ideals of* $A \otimes_K B$ *and ideals of A (Noether-Kurosch) and between intermediate rings of* $A \otimes_K B/B$ *and intermediate rings of A/K.*

Proposition 4.2. *Let P be an algebra over K, A a subalgebra of P, and B a central two-sided simple subalgebra of P. If A and B commute elementwise then* $A \cdot B = A \otimes_K B$.

Proof. The well-defined map $\sum a_i \otimes b_i \longrightarrow \sum a_i b_i$ is an algebra epimorphism $\phi : A \otimes_K B \longrightarrow A \cdot B$. Since $\operatorname{Ker} \phi = \mathfrak{r} \otimes_K B$ with some ideal $\mathfrak{r}$ of A (Lemma 4.1) and $\phi(a) = \phi(a \otimes 1) = a$ for every $a \in A$, we obtain $0 = (\mathfrak{r} \otimes_K B) \cap A = \mathfrak{r}$ (Lemma 4.1), whence it follows $0 = \mathfrak{r} \otimes_K B = \operatorname{Ker} \phi$.

Proposition 4.3. *If A is a two-sided simple algebra over K, and B a central two-sided simple algebra over K then* $A \otimes_K B$ *is also two-sided simple. In particular, if A and B are a simple algebra over K and a central simple algebra over K, respectively, and if one of A and B is finite over K, then* $A \otimes_K B$ *is simple.*

Proof. The first assertion is clear by Lemma 4.1. Concerning the latter, our assumption implies that $A \otimes_K B$ is right Artinian.

Corollary 4.4. *Let D_1 be a central division algebra of finite rank over K, and D_2 a division algebra of finite rank over K. If these two ranks are relatively prime then $D_1 \otimes_K D_1$ is a division ring.*

Proof. Evidently, the capacity n of the simple ring $A = D_1 \otimes_K D_2$ divides $[A:D_2] = [D_1:K]$ and $[A:D_1] = [D_2:K]$ (cf. Prop. 4.3). It follows therefore $n = 1$.

Corollary 4.5. *Let B be a unital simple subring of a simple ring A such that $V = V_A(B)$ is simple, and let C_o be the center of V. If A/B is left locally finite then $B \cdot V$ and every intermediate ring of $B \cdot C_o/B$ are simple rings.*

Proof. Let $Z = V_B(B)$. Since $B \cdot V = B \otimes_Z V$ (Prop. 4.2), V/Z is locally finite. For every simple intermediate ring V' of V/Z with $[V':Z] < \infty$, $B \cdot V'$ is a simple ring (Prop. 4.3). Hence, $B \cdot V$ is simple by Prop. 3.7. Next, for an arbitrary non-zero element $a \in B \cdot C_o$, $BaB \cap C_o$ contains non-zero elements (Lemma 4.1). Hence, every intermediate ring of $B \cdot C_o/B$ is simple again by Prop. 3.7.

Theorem 4.6. *Let A be a central simple algebra over K, B a simple subalgebra of A finite over K, and let B^o be an algebra over K anti-isomorphic to B.*

(a) $A \otimes_K B^o$ and $V_A(B)$ are simple, and the division rings belonging to them are isomorphic.

(b) Every isomorphism of B into A can be extended to an inner automorphism of A.

Proof. By Props. 4.2 and 4.3, $B_L \cdot A_R \simeq A \otimes_K B^o$ is simple. Accordingly, $V_A(B) \simeq E(A_{B_L \cdot A_R})$ is simple by Th. 3.11, and the division ring belonging to $B_L \cdot A_R$ is isomorphic to the one belonging to $E(A_{B_L \cdot A_R})$ by Th. 2.15. Next, we shall prove (b). Let ϕ be an isomorphism of B into A, and $B' = B\phi$. Then ϕ may be regarded as an isomorphism of B_L onto B'_L. By Prop. 4.2, $B_L \cdot A_R = B_L \otimes_K A_R$ and $B'_L \cdot A_R =$

$B'_L \otimes_K A_R$, and then the mapping $\phi \otimes 1$ defined by $\sum b_{iL} \otimes a_{iR} \longrightarrow \sum (b_i \phi)_L \otimes a_{iR}$ is an A_R-isomorphism of $B_L \otimes_K A_R$ onto $B'_L \otimes_K A_R$ that is an extension of ϕ. Since the simple ring $B_L \otimes_K A_R$ is finite over A_R, $\phi \otimes 1$ can be extended to an inner automorphism of $\mathfrak{A} = \mathrm{Hom}(A, A)$: $B_L \otimes_K A_R \mid \theta_L^{-1} \theta_R = \phi \otimes 1$ (Th. 3.11). In particular, $\theta^{-1} y_R \theta = y_R$ for every $y \in A$. It follows therefore $\theta = u_L \in A_L$. Hence, if x is an arbitrary element of B then $u_L^{-1} x_L u_L = \theta^{-1} x_L \theta = (x\phi)_L$, which proves $xu = x\phi$, where $\tilde{u} = u_L u_R^{-1}$.

Writing $B = A$ in Th. 4.6, we obtain the next at once.

Corollary 4.7. *Let A be a central simple algebra of finite rank over K. If A° is anti-isomorphic to A then $A \otimes_K A^\circ$ is isomorphic to the complete matrix ring over K.*

The following is known as a theorem of Wedderburn.

Theorem 4.8. *Let A be a central simple algebra of finite rank over K. If an algebra P over K contains A as a subalgebra then $P = A \cdot V_P(A) = A \otimes_K V_P(A)$.*

Proof. Since $A_L \cdot A_R = A_L \otimes_K A_R$ is simple (Props. 4.2 and 4.3), P is homogeneously A-A-completely reducible: $P = \oplus_\lambda A_\lambda$ with $A_\lambda \simeq A$, where right and left multiplications are considered in P. If $a_\lambda \longleftrightarrow 1$ under the last isomorphism between A_λ and A then $A_\lambda = a_\lambda A$ and a_λ is contained in $V_P(A)$. Hence, $P = A \otimes_K V_P(A)$ (Prop. 4.2).

Corollary 4.9. *Let B be a unital simple subring of A. Let C and Z be the centers of A and of B, respectively. If $[B:Z] < \infty$ and $V_A(B) = C$ then $A = B \otimes_Z C$. In particular, if B is a field and $V_A(B) = C$ then A is commutative.*

Albert [1]; Azumaya [3]; Azumaya-Nakayama [2]; Jacobson [1], [6].

5. Conventions and preliminary results

The present section contains several conventions and preliminary results those which will be used very often in our subsequent study.

Throughout we use the following conventions: A is always a simple ring with the center C, and represented as $\sum_1^n De_{ij}$ with a system of matrix units $E = \{e_{ij}\}$ and the division ring $D = V_A(E)$. B is a unital subring of A, and we set $Z = V_B(B)$, $V = V_A(B)$ and $H = V_A^2(B) = V_A(V)$. The center of V is denoted by C_o. If H is a simple ring, we set $H = \sum Kd_{hk}$ where $\Delta = \{d_{hk}\}$ is a system of matrix units with the division ring $K = V_H(\Delta)$. Further, $\mathfrak{A} = \mathrm{Hom}(A, A)$ (acting on the right side), and $\mathfrak{G}$ denotes the multiplicative group of all B-ring automorphisms of A. If T is an intermediate ring of A/B (resp. a unital subring of A), then $\Gamma(T, A; B)$ (resp. $\Gamma(T, A)$) denotes the set of all B-ring isomorphisms (resp. of all ring isomorphisms) of T into A (sending 1 to 1). For any non-empty subset $\mathfrak{H}$ of $\Gamma(T, A)$, $J(\mathfrak{H})$ means the set $\{t \in T;\ t\sigma = t \text{ for all } \sigma \in \mathfrak{H}\}$, and if S is a subset of T then $\mathfrak{H}(S)$ means the set $\{\sigma \in \mathfrak{H};\ s\sigma = s \text{ for all } s \in S\}$. If V is a simple ring, we set $V = \sum Ug_{pq}$ where $\Gamma = \{g_{pq}\}$ is a system of matrix units with the division ring $U = V_V(\Gamma)$. A unital simple subring of A is called a <u>regular subring</u> of A if the centralizer of the subring in A is simple. In case T is a regular intermediate ring of A/B, $\mathfrak{G}(T, A; B)$ denotes the set of all B-ring isomorphisms of T onto regular subrings of A. By $\mathfrak{R}$ we denote the set of all regular intermediate rings of A/B, and we set $\mathfrak{R}^\circ = \{A' \in \mathfrak{R};\ |A'| = |A|\}$, $\mathfrak{R}_{l.f} = \{A' \in \mathfrak{R};\ A' \text{ is left finite over } B\}$, $\mathfrak{R}_{r.f} = \{A' \in \mathfrak{R};\ A' \text{ is right finite over } B\}$, $\mathfrak{R}^\circ_{l.f} = \mathfrak{R}^\circ \cap \mathfrak{R}_{l.f}$. For any subset S of A, we set $\mathfrak{R}/S = \{A' \in \mathfrak{R};\ A' \supset S\}$, $\mathfrak{R}^\circ/S = \mathfrak{R}^\circ \cap \mathfrak{R}/S$, $\mathfrak{R}_{l.f}/S = \mathfrak{R}_{l.f} \cap \mathfrak{R}/S$ and $\mathfrak{R}^\circ_{l.f}/S = \mathfrak{R}^\circ_{l.f} \cap \mathfrak{R}/S$.

Proposition 5.1. <u>Let</u> B' <u>be a unital subring of</u> A <u>such that</u> A <u>is</u> B'-A-<u>irreducible</u>.

(a) <u>If</u> A' <u>is a simple intermediate ring of</u> A/B' <u>then</u> A' <u>is</u> B'-A'-<u>irreducible</u>.

(b) Let T be an intermediate ring of A/B', and σ in $\Gamma(T, A)$. If for each finite subset F of A there exists a simple intermediate ring A'' of $A/(T\sigma)[F]$ such that $\sigma^{-1} \in T\sigma \mid \Gamma(A'', A)$, then A is $B'\sigma$-A-irreducible.

(c) For each non-zero element $a \in A$, $(B'|a_L)A_R$ is B'_R-A_R-irreducible and canonically isomorphic to A_R.

(d) Let W be a subset of A. If W is right free over $V' = V_A(B')$ then $B'|W_L$ is free over A_R, and conversely. In case W is a subset of A^*, W_L may be replaced by $\widetilde{W} = \{\widetilde{w}; w \in W\}$.

Proof. (a) If a' is an arbitrary non-zero element of A' then $B'a'A' = eA'$ with some non-zero idempotent $e \in A'$. Since $A = B'a'A = B'a'A'A = eA$, e has to be 1.

(b) Let a be an arbitrary non-zero element of A. Then, by assumption, there exists a simple intermediate ring A'' of $A/(T\sigma)[a]$ such that $\sigma^{-1} = T\sigma|\tau$ for some $\tau \in \Gamma(A'', A)$. If $A' = A''\tau$ then A' is B'-A'-irreducible by (a), and so A'' is $B'\sigma$-A''-irreducible. Hence, there holds $\sum x_i a y_i = 1$ with some $x_i \in B'\sigma$ and $y_i \in A''$, which proves the $B'\sigma$-A-irreducibility of A.

(c) The proof is easy and may be left to readers.

(d) Assume first that $B'|W_L$ is not free over A_R. By (c), without loss of generality, we may assume that $B'|w_{1L} = \sum_2^m (B'|w_{iL})x_{iR}$ $(w_i \in W, x_i \in A)$ is a non-trivial relation of the shortest length. If y is an arbitrary element of B' then $0 = y_R(B'|w_{1L}) - (B'|w_{1L})y_R = \sum_2^m (B'|w_{iL})(yx_i - x_i y)_R$, which means that every x_i is contained in V'. Conversely, if W is not right free over V' then some $w_1 \in W$ is represented as $\sum_2^m w_i x_i$ with other w_i's in W $(x_i \in V')$, and then it is evident that $B'|w_{1L} = B'|(\sum_2^m x_{iL}w_{iL}) = \sum_2^m (B'|x_{iR}w_{iL}) = \sum_2^m (B'|w_{iL})x_{iR}$. We have proved thus our first assertion, whence the latter will be easily seen.

Proposition 5.2. Let $\mathfrak{L}'$ be a subring of $\mathfrak{o}$ such that $\mathfrak{L}' \cdot A_R = \mathfrak{L}'$. If A is $V_{\mathfrak{o}}(\mathfrak{L}') \cdot \mathfrak{L}'$-irreducible then $V_{\mathfrak{o}}(\mathfrak{L}')$ is a simple subring of A_L and $V^2_{\mathfrak{o}}(\mathfrak{L}')$ is the closure $\mathrm{Cl}\,\mathfrak{L}'$ of $\mathfrak{L}'$ (in the finite topology).

Proof. Noting that $x\mathfrak{L}'$ $(x \in A)$ is a right A-submodule of A and A is $\mathfrak{L}'$-unital, one will easily see that A contains a minimal $\mathfrak{L}'$-submodule $M = a\mathfrak{L}'$ $(a \in A)$. Since $A = MV_{\mathfrak{A}}(\mathfrak{L}') = \sum_{\alpha \in V_{\mathfrak{A}}(\mathfrak{L}')} M\alpha$ and $M\alpha$ is either $\mathfrak{L}'$-isomorphic to M or 0, A is homogeneously $\mathfrak{L}'$-completely reducible. Hence, $V_{\mathfrak{A}}(\mathfrak{L}')$ is simple, and $\mathfrak{L}'$ is dense in $V^2_{\mathfrak{A}}(\mathfrak{L}')$ $(\ni 1)$ by Th. 2.5. Now, one will easily see that $V_{\mathfrak{A}}(\mathfrak{L}') \subset A_L$.

The converse of Prop. 5.2 will be rather familiar: Let B' be a unital subring of A such that B' is a direct summand of the left B'-module A (or ${}_{B'}A$ is completely faithful (Prop. 2.12)). If a subring $\mathfrak{L}'$ of $\mathfrak{A}$ is dense in $V_{\mathfrak{A}}(B'_L)$ then $B'_L = V_{\mathfrak{A}}(\mathfrak{L}')$ by Th. 2.13. In particular, if $\mathfrak{G}'$ is the group of all B'-ring automorphisms of A and $\mathfrak{G}'A_R$ is dense in $V_{\mathfrak{A}}(B'_L)$ then $J(\mathfrak{G}') = B'$. Further, if B' is simple and a subring $\mathfrak{L}'$ of $\mathfrak{A}$ is dense in $V_{\mathfrak{A}}(B'_L)$ then it turns out that A is $V_{\mathfrak{A}}(\mathfrak{L}')\cdot\mathfrak{L}'$-irreducible (cf. Prop. 2.3 (b)). Accordingly, combining the above with Prop. 5.2, we obtain the following:

Corollary 5.3. *The correspondences* $\mathfrak{L}' \longrightarrow (1)V_{\mathfrak{A}}(\mathfrak{L}')$ *and* $B' \longrightarrow V_{\mathfrak{A}}(B'_L)$ *are mutually converse* 1-1 *dual correspondences between closed intermediate rings* $\mathfrak{L}'$ *of* $\mathfrak{A}/A_R$ *such that* A *is* $V_{\mathfrak{A}}(\mathfrak{L}')\cdot\mathfrak{L}'$-*irreducible and unital simple subrings* B' *of* A.

The first assertion of the following is an easy consequence of Prop. 5.2.

Proposition 5.4. *Let* B' *be a unital subring of* A, $V' = V_A(B')$ *and* $H' = V^2_A(B')$.

(a) *If* A *is* $B'\cdot V'$-A-*irreducible then* A *is homogeneously completely reducible as* B'-A-*module and as* V'-A-*module, both* V' *and* H' *are simple rings,* $[A|B'_L\cdot A_R] = |V'|$ *and* $[A|V'_L\cdot A_R] = |H'|$.

(b) *If* B *is a unital simple subring of* B' *with* $[B':B]_L < \infty$ *and* A *is* $B'\cdot V'$-A-*irreducible, then* $[V:V']_R \leq [B':B]_L$. *If moreover* A/B *is left locally finite then* $[V:V']_L \leq [B':B]_L$.

Proof. We shall prove (b). Let $V' = \sum_1^s U'g'_{pq}$, where $\Gamma' = \{g'_{pq}\}$ is a system of matrix units with the division ring $U' = V_{V'}(\Gamma')$. Then, Γ' forms a B'-basis of $\bar{B} = B'[\Gamma']$. Since $\bar{B}\cdot V_A(\bar{B}) = \bar{B}\cdot U' = B'\cdot V'$, A is $\bar{B}$-A-irreducible by (a). It follows therefore $\infty > [\bar{B}:B]_L = [\mathrm{Hom}({}_B\bar{B}, {}_BA):A_R]_R \geqq [(\bar{B}|V_L)A_R:A_R]_R = [V:U']_R$ (Prop. 5.1 (d)), whence it follows $[V:V']_R\cdot s^2 \leqq s^2\cdot[B':B]_L$, and eventually $[V:V']_R \leqq [B':B]_L$. In what follows, we assume that A/B is left locally finite. For an arbitrary finite subset X of V that is free over V', we set $B'' = \bar{B}[X, E]$ ($\in \mathfrak{K}^{\circ}_{l.f}$), $V^* = V_{B''}(B)$, $V'' = V_{B''}(B')$ (simple) and $C'' = V_{B''}(B'')$. Then, B'' being B''-B''-irreducible, $[V^*:C''] \leqq [B'':B]_L < \infty$ by the fact proved above, and therefore $[V^*:V'']_L = [V^*:V'']_R < \infty$. Further, as B'' is ($\bar{B}$-B''-irreducible by Prop. 5.1 (a), and so) $B'\cdot V''$-B''-irreducible, we obtain $[V^*:V'']_R \leqq [B':B]_L$ again by the fact proved above. Hence, $\#X \leqq [V^*:V'']_L = [V^*:V'']_R \leqq [B':B]_L$, which proves $[V:V']_L \leqq [B':B]_L$.

Corollary 5.5. Let A be $B\cdot V$-A-irreducible.

(a) If T is an intermediate ring of A/H such that A is T-A-irreducible then $[V:V_A(T)]_R = [T:H]_L$, provided we do not distinguish between two infinite dimensions.

(b) Let B be a simple ring. If B' is an intermediate ring of A/B left finite over B such that A is B'-A-irreducible, then $[V_A^2(B'):H]_L = [V:V_A(B')]_R < \infty$ and $V_A^2(B') = H[B']$.

(c) Let B be a simple ring. If B' is an intermediate ring of A/B right finite over B such that A is A-B'-irreducible, then $[V_A^2(B'):H]_R = [V:V_A(B')]_L < \infty$ and $V_A^2(B') = H[B']$.

(d) Let B be a simple ring. If A/B is left (resp. right) locally finite then A/H is left (resp. right) locally finite.

Proof. By Prop. 5.4 (a), V and H are simple rings. Moreover, (d) is an easy consequence of (b) or (c).

(a) Since $V_L\cdot A_R$ is dense in $\mathrm{Hom}({}_HA, {}_HA)$ by Prop. 5.2, one will easily see that $[(T|V_L)A_R:A_R]_R = [T:H]_L$ provided we do not distinguish between two infinite dimensions (Prop. 5.1 (c)). On the other

hand, $[(T|V_L)A_R:A_R]_R = [V:V_A(T)]_R$ by Prop. 5.1 (d). Combining those, it follows at once our assertion.

(b) Obviously, $H \subset H[B'] \subset V_A^2(B')$ and A is $H[B']$-A-irreducible. Since $V_A(H[B']) = V_A(V_A^2(B'))$ and $\infty > [B':B]_L \geqslant [V:V_A(B')]_R$ by Prop. 5.4 (b), (a) implies that $\infty > [V_A^2(B'):H]_L = [V:V_A(B')]_R = [H[B']:H]_L$.

(c) By Prop. 5.4 (b), we obtain $\infty > [B':B]_R \geqslant [V:V_A(B')]_L \geqslant [V_A^2(B'):H]_R \geqslant [H[B']:H]_R \geqslant [V:V_A(B')]_L$, namely, $\infty > [V:V_A(B')]_L = [V_A^2(B'):H]_R = [H[B']:H]_R$.

Corollary 5.6. Let A be $B \cdot V$-A-irreducible.

(a) If $\mathfrak{H}$ is a subset of $\mathfrak{o}$ containing $\widetilde{V}$ such that $V_{\mathfrak{o}}(\mathfrak{H}) \cap A_L = B_L$ then B is a simple ring and $A_R[\mathfrak{H}]$ is dense in $V_{\mathfrak{o}}(B_L)$.

(b) If $\mathfrak{H}$ is a subgroup of $\mathfrak{o}$ containing $\widetilde{V}$ and $J(\mathfrak{H}) = B$ then B is simple, $\mathfrak{H}A_R$ is dense in $V_{\mathfrak{o}}(B_L)$ and $(H|\mathfrak{H})H_R$ is dense in $\mathrm{Hom}({}_BH, {}_BH)$.

Proof. Again by Prop. 5.4 (a), V and H are simple rings.

(a) Since $A_R[\mathfrak{H}] \supset \widetilde{V}A_R = V_L \cdot A_R$, our assertion is clear by Prop. 5.2.

(b) By the validity of (a), it suffices to prove the last assertion. Let h be an arbitrary non-zero element of H. Then, $(Bh)\mathfrak{H}H_R = eH$ with some non-zero idempotent e. Since $A = (Bh)\mathfrak{H}A_R = ((Bh)\mathfrak{H}H_R)A_R = eA$, e has to be 1. Hence, H is $B_L \cdot (H|\mathfrak{H})H_R$-irreducible. Consequently, again by Prop. 5.2, $(H|\mathfrak{H})H_R$ is dense in $\mathrm{Hom}({}_BH, {}_BH)$.

Proposition 5.7. Let $T \supset B'$ be intermediate rings of A/B, and $\mathfrak{H}$ a subset of $\Gamma(T, A; B)$ such that A is $B'\sigma$-A-irreducible for every σ in $\mathfrak{H}$.

(a) Let M be a non-zero right B'-submodule of T, and σ in $\mathfrak{H}$. Then, $(M|\sigma)A_R$ is B_R'-A_R-irreducible and canonically A_R-isomorphic to A_R.

(b) Let M be a non-zero (right) B'-submodule of T, and $\mathfrak{H}'$ a subset of $\mathfrak{H}$. If $M|\mathfrak{H}'$ is V_R-free then it is A_R-free, and conversely.

Accordingly, in order that $M|\mathfrak{H}'$ form an A_R-basis of $(M|\mathfrak{H})A_R$, it is necessary and sufficient that $M|\mathfrak{H}'$ form a V_R-basis of $(M|\mathfrak{H})V_R$.

(c) Let $\mathfrak{m}$ be a B'_R-A_R-submodule of $(B'|\mathfrak{H})A_R$. In order that $\mathfrak{m}$ be B'_R-A_R-irreducible, it is necessary and sufficient that $\mathfrak{m} = (B'|\sigma u_L)A_R$ with some $\sigma \in \mathfrak{H}$ and non-zero $u \in V$.

(d) Let α be a B-ring homomorphism of B' into A, and σ in $\mathfrak{H}$. If αA_R is B'_R-A_R-isomorphic to $(B'|\sigma)A_R$ then $\alpha = B'|\sigma\tilde{v}$ with some $v \in V^*$, and conversely. Accordingly, if α is contained in $(B'|\mathfrak{H})A_R$ then $\alpha = B'|\tau\tilde{u}$ with some $\tau \in \mathfrak{H}$ and $u \in V^*$.

(e) If $\mathfrak{H}\tilde{V} = \mathfrak{H}$ then each homogeneous component of $(B'|\mathfrak{H})A_R$ as B'_R-A_R-module is of the form $(B'|\sigma\tilde{V})A_R$ with $\sigma \in \mathfrak{H}$.

Proof. (a) Given an arbitrary non-zero element $a \in A$, we obtain $B'_R(M|\sigma)a_R A_R = (M|\sigma)(B'\sigma \cdot aA)_R = (M|\sigma)A_R$, which means evidently the B'_R-A_R-irreducibility of $(M|\sigma)A_R$. The canonical isomorphism is now obvious.

(b) If $M|\mathfrak{H}'$ is (not) A_R-free, by the validity of (a) we may assume that $M|\sigma_1 = \sum_2^t (M|\sigma_i)a_{iR}$ ($\sigma_i \in \mathfrak{H}'$, $a_i \in A$) is a non-trivial relation of the shortest length. Then, for each $b \in B$ there holds $0 = b_R(M|\sigma_1) - (M|\sigma_1)b_R = \sum_2^t (M|\sigma_i)(ba_i - a_i b)_R$, whence it follows $ba_i = a_i b$, namely, $a_i \in V$ ($i = 2, \ldots, t$). The remaining is obvious.

(c) There exists some $\sigma \in \mathfrak{H}$ such that $(B'|\sigma)A_R$ is B'_R-A_R-isomorphic to $\mathfrak{m}$ (cf. (a)). If $B'|\sigma \longleftrightarrow \alpha$ ($\in \mathfrak{m}$), then $\mathfrak{m} = \alpha A_R$. For each $x \in B'$ there hold $x_R(B'|\sigma) \longleftrightarrow x_R\alpha$ and $(B'|\sigma)(x\sigma)_R \longleftrightarrow \alpha(x\sigma)_R$. It follows therefore $x_R\alpha = \alpha(x\sigma)_R$. Applying the both sides to $1 \in B'$, we obtain $x\alpha = 1\alpha \cdot x\sigma$, that is, $\alpha = B'|\sigma(1\alpha)_L$.

(d) Let $(B'|\sigma)A_R$ be B'_R-A_R-isomorphic to αA_R, and $B'|\sigma \longleftrightarrow \alpha v_R$ under the isomorphism. Then, v is contained in V. Applying the both sides of $\alpha v_R A_R = \alpha A_R$ to $1 \in B'$, we see that $vA = A$, which implies $v \in V^*$. Now, for each $x \in B'$, there holds $x_R\alpha v_R \longleftrightarrow x_R(B'|\sigma) = (B'|\sigma)(x\sigma)_R \longleftrightarrow \alpha v_R(x\sigma)_R$, whence it follows

$x_R\alpha\, v_R = \alpha v_R(x\sigma)_R$. Again applying the both sides to $1 \in B'$, we obtain $(x\alpha)v = v(x\sigma)$, and eventually $\alpha = B'|\sigma\tilde{v}$. The converse is almost evident by the above proof, and the latter assertion is now obvious by (a).

(e) This is a direct consequence of (a) and (d).

The assumption in Prop. 5.7 will be often specialized to be the following:

(1) Let B' be in $\mathfrak{R}^\circ$, T an intermediate ring of A/B', and $\mathfrak{G}$ a subset of $\mathfrak{J}(T, A; B)$.

(2) Let B' be an intermediate ring of A/B such that A is B'-A-irreducible, and $\mathfrak{G}$ a subset of $\mathfrak{J}$ (and $T = A$).

(3) Assume that A is left locally finite over a unital simple subring B and $T_2 | \mathfrak{J}(T_1, A; B) = \mathfrak{J}(T_2, A; B)$ for each $T_1 \supset T_2$ in $\mathfrak{R}^\circ_{l.f}$. Let B' be an intermediate ring of A/B such that A is B'-A-irreducible and $[B':B]_L < \infty$, T in $\mathfrak{R}^\circ_{l.f}/B'$, and $\mathfrak{G}$ a subset of $\mathfrak{J}(T, A; B)$ (cf. Prop. 5.1 (b)).

Let $\mathfrak{G}$ be a (multiplicative) sub-semigroup of $\mathfrak{V}$. If $\mathfrak{G}A_R$ and $\mathfrak{G}A_L$ form subrings of $\mathfrak{V}$ (or, $A_R\mathfrak{G} \subset \mathfrak{G}A_R$ and $A_L\mathfrak{G} \subset \mathfrak{G}A_L$) and $V_{\mathfrak{V}}(\mathfrak{G}) \cap A_R = B_R$ and $V_{\mathfrak{V}}(\mathfrak{G}) \cap A_L = B_L$, then $\mathfrak{G}$ is called a <u>Galois semigroup of</u> A/B.

Lemma 5.8. <u>Let</u> A <u>be</u> B·V-A-<u>irreducible, and</u> $\mathfrak{G}$ <u>a Galois semigroup of</u> A/B <u>containing</u> $\tilde{V}$. <u>Let</u> T <u>be a</u> B-B-<u>submodule of</u> A.

(a) <u>If</u> T <u>is left finite over</u> B <u>then</u> $(T|\mathfrak{G})V_R$ <u>possesses a</u> V_R-<u>basis that forms at the same time an</u> A_R-<u>basis of</u> $(T|\mathfrak{G})A_R$.

(b) <u>In order that</u> T <u>be left finite over</u> B, <u>it is necessary and sufficient that</u> $[(T|\mathfrak{G})V_R|V_R]$ <u>be finite</u>.

Proof. By Cor. 5.6 (a), B is regular and $\mathfrak{G}A_R$ is dense in $V_{\mathfrak{V}}(B_L)$. Moreover, by Prop. 3.4, T has a left free B-basis.

(a) If $g_p = g_{pp}$ then $A = \oplus_1^r g_pA$ and g_{qpL} induces a B-A-isomorphism of g_pA onto g_qA. Since A is homogeneously B-A-completely reducible and $[A|B_L \cdot A_R] = |V| = r$ (Prop. 5.4 (a)), g_pA is

B-A-irreducible, and hence $(g_pA)_R$ is B_R-A_R-irreducible. Accordingly, $(T|\sigma)(g_pA)_R$ being B_R-A_R-homomorphic to $(g_pA)_R$ for every $\sigma \in \mathfrak{G}$, $\mathrm{Hom}({}_BT, {}_BA) = \oplus_1^s (T|\sigma_\lambda)(g'_\lambda A)_R$ with some $\sigma_\lambda \in \mathfrak{G}$ and $g'_\lambda \in \{g_p\}$, where each $(T|\sigma_\lambda)(g'_\lambda A)_R$ is B_R-A_R-isomorphic to arbitrary fixed $(g_pA)_R$. Recalling here that $A = \oplus_1^r g_pA$, the last relation yields $s = r\cdot[T:B]_L$, and so $\mathfrak{T} = \sum_\lambda (T|\sigma_\lambda)(g'_\lambda V)_R = \oplus_\lambda (T|\sigma_\lambda)(g'_\lambda V)_R$ possesses a V_R-basis $\{\varepsilon_1, \ldots, \varepsilon_t\}$ and $[\mathfrak{T}:V_R]_R = [T:B]_L$. Since $(T|\mathfrak{G})A_R = \mathfrak{T}A_R$ and $[(T|\mathfrak{G})A_R:A_R]_R = [T:B]_L$, the V_R-basis $\{\varepsilon_1, \ldots, \varepsilon_t\}$ is still an A_R-basis of $(T|\mathfrak{G})A_R$. Now, one will easily see that $\mathfrak{T} = \mathrm{Hom}({}_BT_B, {}_BA_B) = (T|\mathfrak{G})V_R$.

(b) Since $\mathfrak{G}A_R$ is dense in $V_{\mathfrak{o}\mathfrak{l}}(B_L)$, this is a consequence of (a).

Proposition 5.9. Assume that A is $B\cdot V$-A-irreducible and A-$B\cdot V$-irreducible. Let $\mathfrak{G}$ be a Galois semigroup of A/B containing $\tilde{V}$. Let T be a B-B-submodule of A possessing a finite left B-basis ~~and a right B-basis~~, and $\{\varepsilon_1, \ldots, \varepsilon_t\}$ a V_R-basis of $(T|\mathfrak{G})V_R$ that forms at the same time an A_R-basis of $(T|\mathfrak{G})A_R$ (cf. Lemma 5.8 (a)). If $V_A(\cup_1^t T\varepsilon_i) \cap V$ contains a unital division subring U' such that $[V:U']_L < \infty$ then $[T:B]_R \leqq [T:B]_L$.

Proof. By Cor. 5.6 (a), B is regular, $\mathfrak{G}A_R$ and $\mathfrak{G}A_L$ are dense in $V_{\mathfrak{o}\mathfrak{l}}(B_L)$ and $V_{\mathfrak{o}\mathfrak{l}}(B_R)$, respectively. Hence $\mathrm{Hom}({}_BT, {}_BA) = (T|\mathfrak{G})A_R = \oplus_1^t \varepsilon_i A_R$ $(t = [T:B]_L)$. Moreover, one will easily see that $\mathfrak{T} = \oplus_1^t \varepsilon_i V_R = \mathrm{Hom}({}_BT_B, {}_BA_B) \supset (T|\mathfrak{G})V_L$. If $\{v_1, \ldots, v_m\}$ is a left U'-basis of V then by the assumption we have $\mathfrak{T} = \sum_{i=1}^t \varepsilon_i(\sum_{k=1}^m U'_R v_{kR}) = \sum_{i,k} \varepsilon_i v_{kR} U'_L$. Hence, $tm \geqslant [\mathfrak{T}:U'_L]_R$, and then $[(T|\mathfrak{G})V_L|V_L]$ is finite. Accordingly, by the proposition symmetric to Lemma 5.8, it follows $\infty > [T:B]_R = [(T|\mathfrak{G})V_L:V_L]_R$. Then, noting that $[\mathfrak{T}:U'_L]_R = [\mathfrak{T}|V_L]\cdot(m/|V|)$, we readily obtain $t \geqslant [\mathfrak{T}|V_L]/|V| \geqslant [(T|\mathfrak{G})V_L|V_L]/|V| = [T:B]_R$.

Nagahara [8], [10]; Nagahara-Tominaga [8], [9]; Tominaga [10], [11].

6. w-q-Galois extension

In this section, we shall develop a kind of preliminary Galois theory of simple rings. If B is simple and $\mathrm{Hom}({}_BT, {}_BA) = \mathcal{G}(T, A; B)A_R$ for every $T \in \mathcal{R}^{\circ}_{l.f}$ then A/B is said to be w-q-Galois. The next theorem will be a key result for the construction of Galois theory of simple rings.

Theorem 6.1. *Let A/B be w-q-Galois and left locally finite.*

(a) *If B' is a simple intermediate ring of A/B with $[B':B]_L < \infty$ then for any finite subset F of A there exists some T' in $\mathcal{R}^{\circ}_{l.f}/B'[F]$ such that each intermediate ring A' of A/T' is B'-A'-completely reducible.*

(b) *If B' is in $\mathcal{R}_{l.f}$ then for any finite subset F of A there exists some T' in $\mathcal{R}^{\circ}_{l.f}/B'[F]$ such that each intermediate ring A' of A/T' is homogeneously B'-A'-completely reducible, and $[A'|B'_L \cdot A'_R] = |V_A(B')|$ and $[V_{A'}(B):V_{A'}(B')]_R < \infty$.*

Proof. (a) Let M be a minimal B'-A-submodule of A such that the composition series of M as A-module is of the shortest length among minimal B'-A-submodules of A. Then, $M = eA$ with a non-zero idempotent e. In virtue of Prop. 3.6 (b), we can find a T^* in $\mathcal{R}^{\circ}_{l.f}/B'[e, F]$ such that $[eT^*|T^*] = [M|A]$. One may remark here that eT^* is a B'-T^*-submodule of T^*. Since $\mathrm{Hom}({}_BT^*, {}_BA) = \mathcal{G}(T^*, A; B)A_R = \sum_1^s \tau_i A_R$ with some $\tau_i \in \mathcal{G}(T^*, A; B)$, there exists some T' in $\mathcal{R}^{\circ}_{l.f}/T^*$ such that $\mathrm{Hom}({}_BT^*, {}_BA') = \mathcal{G}(T^*, A'; B)A'_R$ for every intermediate ring A' of A/T'. By the above remark $B'eT^* = eT^*$ and Prop. 3.6 (b), one will see that $M' = eA'$ is a (minimal) B'-A'-submodule of A' such that the length of the composition series of M' as A'-module coincides with $[M|A] = [eT^*|T^*]$ (and so $[M'|A'] \leqq [N'|A']$ for every non-zero B'-A'-submodule N' of A'). Since $\mathrm{Hom}({}_BT^*, {}_BA')$ is T^*_R-A'_R-completely reducible by Prop. 5.7 (a), the T^*_R-A'_R-submodule $\mathrm{Hom}({}_{B'}T^*, {}_{B'}A') = \oplus_1^t \mathfrak{m}_j$ with some irreducible $\mathfrak{m}_j$'s. By Prop. 5.7 (c), $\mathfrak{m}_j = \sigma_j u_j L A'_R$ with some $\sigma_j \in \mathcal{G}(T^*, A'; B)$ and non-zero $u_j \in V_{A'}(B)$. Since $\mathfrak{m}_j$ is contained in $\mathrm{Hom}({}_{B'}T^*, {}_{B'}A')$

and $B'e \subset eT^* \subset T^*$, each $M_j = (B'e)\mathfrak{m}_j$ is a B'-A'-submodule of A'. Further, there holds $M_j = u_j \cdot (B'e)\sigma_j \cdot A' = u_j \cdot (B'eT^*)\sigma_j \cdot A' = u_j \cdot (eT^*)\sigma_j \cdot A' = u_j \cdot e\sigma_j \cdot A'$, whence it follows $[M_j|A'] = [u_j \cdot e\sigma_j \cdot A'|A'] \leqq [e\sigma_j \cdot A'|A'] \leqq [e\sigma_j \cdot T^*\sigma_j|T^*\sigma_j] = [eT^*|T^*] = [M'|A']$ by Prop. 3.6 (b). Recalling here that $[M'|A']$ is the least, we see that each M_j is either 0 or B'-A'-irreducible. Finally, noting that A' is $B'_L \cdot \mathrm{Hom}({}_{B'}A', {}_{B'}A')$-irreducible, there holds $A' = e(B'_L \cdot \mathrm{Hom}({}_{B'}A', {}_{B'}A')) = (B'e)\mathrm{Hom}({}_{B'}T^*, {}_{B'}A') = (B'e)\sum_1^t \mathfrak{m}_j = \sum_1^t M_j$, which proves evidently the complete reducibility of A' as B'-A'-module.

(b) Let $V' = V_A(B') = \sum U'g'_{pq}$, where $\Gamma' = \{g'_{pq}\}$ is a system of matrix units and $U' = V_{V'}(\Gamma')$ a division ring. By (a), there exists some $T' \in \mathfrak{R}^{\circ}_{l.f}/B'[\Gamma', F]$ such that every intermediate ring A' of A/T' is B'-A'-completely reducible. Since $\mathrm{Hom}({}_{B'}A'_{A'}, {}_{B'}A'_{A'})$ coincides with the simple ring $(V_{A'}(B'))_L$, A' is B'-A'-homogeneous and $[A'|B'_L \cdot A'_R] = |V_{A'}(B')| = |V'|$. Accordingly, A' is $B' \cdot V_{A'}(B')$-A'-irreducible, and hence $\infty > [B':B]_L \geqslant [V_{A'}(B):V_{A'}(B')]_R$ (Prop. 5.4 (b)).

Corollary 6.2. Let A/B be w-q-Galois and left locally finite. If V is a division ring then every intermediate ring of A/B is simple, and conversely.

Proof. By Th. 6.1 (b), A is B-A-irreducible. Hence, every intermediate ring of A/B is simple by Prop. 3.8 (b). The converse part is valid even under the assumption that A is left algebraic over the simple ring B and every intermediate ring of A/B left finite over B is simple. In fact, for an arbitrary non-zero element $v \in V$, $B[v]$ is simple, and so the center of $B[v]$ is a field. Hence, v belonging to the center of $B[v]$ is a unit and v^{-1} is contained in V.

The next is often efficient in our subsequent study.

Theorem 6.3. Let A/B be w-q-Galois and left locally finite. If A^* is in $\mathfrak{R}$ then A^* contains a subring B^* such that $B^*[F^*]$ is in $\mathfrak{R}_{l.f}$ for every finite subset F^* of A^*.

Proof. Let $A^* = \sum D^* e^*_{ij}$ and $V^* = V_A(A^*) = \sum U^* g^*_{pq}$, where $E^* = \{e^*_{ij}\}$ and $\Gamma^* = \{g^*_{pq}\}$ are systems of matrix units with the division rings $D^* = V_{A^*}(E^*)$ and $U^* = V_{V^*}(\Gamma^*)$, respectively. Then $A^{**} = A^*[\Gamma^*] = \sum A^* g^*_{pq} = \sum D^* e^*_{ij} \cdot g^*_{pq}$, where $E^* \cdot \Gamma^* = \{e^*_{ij} \cdot g^*_{pq}\}$ forms evidently a system of matrix units and $V_{A^{**}}(E^* \cdot \Gamma^*) = D^*$. Accordingly, for an arbitrary finite subset F of A^{**}, $B_F = B[E^*, \Gamma^*, F]$ is a simple subring of A^{**} with $[B_F : B]_L < \infty$. As A is B_F-A-completely reducible by Th. 6.1, we shall denote by $n(F)$ the length of its composition series, that is evidently bounded with the capacity n of A. Now, we set $n(F') = \min n(F)$, where F ranges over all the finite subsets of A^{**}. We assume in below F is an arbitrary finite subset of A^{**} containing F' and $A = N_1 \oplus \dots \oplus N_{n(F)}$ is a direct decomposition of A into B_F-A-irreducible submodules. Since each N_i is yet $B_{F'}$-A-admissible, we have $n(F) \leqslant n(F')$, whence it follows $n(F) = n(F')$. Hence, we see that each N_i is $B_{F'}$-A-irreducible, and so if $A = M_1 \oplus \dots \oplus M_t$ is the idealistic decomposition of the $B_{F'}$-A-module A then every M_j is B_F-A-admissible, which means that each M_j is A^{**}-A-admissible. As $V_A(A^{**}) = U^*$ is a division ring, t is to be 1, namely, A is homogeneously $B_{F'}$-A-completely reducible. Further, by the same reason, $n(F) = n(F')$ implies that A is homogeneously B_F-A-completely reducible, and hence $V_A(B_F)$ is a simple ring. Evidently, $B'_F = V_{B_F}(\Gamma^*)$ is a simple subring of $A^* = V_{A^{**}}(\Gamma^*)$ containing B with $[B'_F : B]_L < \infty$, and it is easy to see that $V_A(B'_F) = \sum V_A(B_F) g^*_{pq}$, which proves that B'_F is in $\mathfrak{L}_{l.f}$. Now, noting that $B'_{F'}[F^*] = B'_{F' \cup F^*}$ for any finite subset F^* of A^*, it is obvious that $B'_{F'}$ can be taken as our B^*.

Lemma 6.4. *Let A/B be w-q-Galois and left locally finite.*

(a) *If ρ is a B-ring homomorphism of an intermediate ring A_1 of A/B with $[A_1 : B]_L < \infty$ into A such that A is $A_1\rho$-A-irreducible, then ρ is contained in $A_1|\mathfrak{G}(A_0, A; B)$ for every A_0*

in $\mathfrak{R}^{\circ}_{1.f}/A_1$.

(b) If B' is in $\mathfrak{R}_{1.f}$ then $B'|\mathcal{G}(T, A; B) \subset \mathcal{G}(B', A; B)$ for every $T \in \mathfrak{R}^{\circ}_{1.f}/B'$.

Proof. (a) If $\mathcal{G} = \mathcal{G}(A_o, A; B)$ then $\mathrm{Hom}({}_BA_1, {}_BA) = (A_1|\mathcal{G})A_R = \sum_1^s (A_1|\sigma_i)A_R$ with some $\sigma_i \in \mathcal{G}$. Now, ρ can be represented as a linear combination of these $A_1|\sigma_i$ with coefficients in A_R, and we may assume without loss of generality that $\rho = \sum_1^t (A_1|\sigma_i)a_{iR}$ $(a_i \neq 0)$ is a representation of the shortest length. Recalling that A is $A_1\rho$-A-irreducible, for each non-zero a in A we have $A_{1R}\rho a_R A_R = \rho(A_1\rho \cdot aA)_R = \rho A_R \ni \rho$. Thus, we see that ρa_R is not contained in $\sum_2^t (A_1|\sigma_i)A_R$, provided a is a non-zero element of A. Particularly, we see that a_1 is in A^*. Accordingly, it follows that $\rho a_{1R}^{-1} = (A_1|\sigma_1) + \sum_2^t (A_1|\sigma_i)\cdot(a_i a_1^{-1})_R$. Now, for an arbitrary $x \in A_1$, there holds $\rho(x\rho \cdot a_1^{-1} - a_1^{-1}\cdot x\sigma_1)_R = x_R\rho a_{1R}^{-1} - \rho a_{1R}^{-1}(x\sigma_1)_R = \sum_2^t (A_1|\sigma_i)\{x\sigma_i \cdot a_i a_1^{-1} - a_i a_1^{-1}\cdot x\sigma_1\}_R$. By the remark cited above, it follows then $x\rho \cdot a_1^{-1} - a_1^{-1}\cdot x\sigma_1 = 0$, which means $\rho a_{1R}^{-1} = (A_1|\sigma_1)a_{1L}^{-1}$. We have proved therefore that $\rho = A_1|\sigma_1\tilde{a}_1^{-1}$. Evidently, $\sigma_1\tilde{a}_1^{-1}$ is contained in $\mathcal{G}(A_o, A; B)$.

(b) Let $V' = V_A(B') = \sum U'g'_{pq}$, where $\Gamma' = \{g'_{pq}\}$ is a system of matrix units and $U' = V_{V'}(\Gamma')$ a division ring. We set $\bar{B} = B'[\Gamma']$ and $\bar{T} = T[\Gamma']$. Now, let σ be an arbitrary element of $\mathcal{G}(T, A; B)$. By (a), $\sigma = T|\bar{\sigma}$ for some $\bar{\sigma} \in \mathcal{G}(\bar{T}, A; B)$. Obviously, $V_A(B'\sigma) = V_A(B'\bar{\sigma})$ contains $\Gamma'\bar{\sigma}$ as a system of matrix units and the centralizer of $\Gamma'\bar{\sigma}$ in $V_A(B'\sigma)$ coincides with $V_A(\bar{B}\bar{\sigma})$. If a is in $V_A(\bar{B}\bar{\sigma})$ and $T^* = (\bar{T}\bar{\sigma})[a]$ $(\in \mathfrak{R}^{\circ}_{1.f})$, then $\bar{\sigma}^{-1} = \bar{T}\bar{\sigma}|\tau^*$ for some $\tau^* \in \mathcal{G}(T^*, A; B)$ again by (a). For any $x \in \bar{B}$, the equality $x\bar{\sigma}\cdot a = a\cdot x\bar{\sigma}$ yields $x\cdot a\tau^* = a\tau^*\cdot x$. Hence, $a\tau^*$ is contained in the division ring $V_A(\bar{B}) = U'$. Accordingly, $a\tau^*$ is a unit of $T^*\tau^*$, and so a is a unit. We have proved thus $V_A(\bar{B}\bar{\sigma})$ is a division ring, which implies that $V_A(B'\sigma) = \sum V_A(\bar{B}\bar{\sigma})\cdot g'_{pq}\bar{\sigma}$ is a simple ring.

Theorem 6.5. Let A be w-q-Galois and left locally finite over B.

(a) $B_2 \mid \mathfrak{G}(B_1, A; B) = \mathfrak{G}(B_2, A; B)$ for every $B_1 \supset B_2$ in $\mathfrak{R}_{1.f}$.

(b) If B_2 is in $\mathfrak{R}_{1.f}$ then $B_2 \mid \mathfrak{G}(A', A; B) \subset \mathfrak{G}(B_2, A; B)$ for every $A' \in \mathfrak{R}/B_2$ and $|V_A(B_2\sigma')| = |V_A(B_2)|$ for every σ' in $\mathfrak{G}(A', A; B)$.

(c) Let A' be in $\mathfrak{R}$. If σ' is in $\mathfrak{G}(A', A; B)$ then $(A' \cap H)\sigma' = A'\sigma' \cap H$.

Proof. (a) Let σ be an arbitrary element of $\mathfrak{G}(B_2, A; B)$, and $B_3 = B_2\sigma$. We set $V_i = V_A(B_i) = \sum_1^{m_i} U_i g_{pq}^{(i)}$ $(i = 2, 3)$, where $\{g_{pq}^{(i)}\}$ is a system of matrix units with the division ring $U_i = V_{V_i}(\{g_{pq}^{(i)}\})$. If $m_2 \geqslant m_3$, we can consider the subrings A_2, A_3 of A defined as follows: $A_2 = \sum_1^{m_3} B_2 g_{pq}^{(2)} + B_2 g$ where $g = \sum_{m_3+1}^{m_2} g_{pp}^{(2)}$, and $A_3 = \sum_1^{m_3} B_3 g_{pq}^{(3)}$. Evidently, A_2 is an intermediate ring of A/B_2 left finite over B, A_3 a simple intermediate ring of A/B_3, and $V_A(A_3) = U_3$ a division ring. As $\{g_{pq}^{(i)}\}$ is free over B_i, we can define a B-linear map ρ of A_2 onto A_3 by the following rules: $(B_2 g)\rho = 0$ and $(\sum_1^{m_3} b_{pq}^{(2)} g_{pq}^{(2)})\rho = \sum_1^{m_3} (b_{pq}^{(2)}\sigma) g_{pq}^{(3)}$ $(b_{pq}^{(2)} \in B_2)$. Then, one will readily see that ρ is a ring homomorphism and $B_2|\rho$ coincides with σ. Now, let A_o be an arbitrary member of $\mathfrak{R}^{\circ}_{1.f}/A_2[B_1]$. Since A is A_3-A-irreducible (Th. 6.1 (b)), $\rho = A_2|\tau$ with some $\tau \in \mathfrak{G}(A_o, A; B)$ (Lemma 6.4 (a)). Then, as was shown in the proof of Lemma 6.4 (b), we obtain $m_2 = m_3$. Moreover, we have

$$\sigma = B_2|\rho \in B_2|\mathfrak{G}(A_o, A; B) = B_2|(B_1|\mathfrak{G}(A_o, A; B)) \subset B_2|\mathfrak{G}(B_1, A; B)$$

by Lemma 6.4 (b), namely, $\mathfrak{G}(B_2, A; B) \subset B_2|\mathfrak{G}(B_1, A; B)$. Whereas, if $m_3 \geqslant m_2$, the same argument applied to σ^{-1} (instead of σ) enables us to see that $m_3 = m_2$. Hence, there holds always that $m_2 = m_3$ and $\mathfrak{G}(B_2, A; B) \subset B_2|\mathfrak{G}(B_1, A; B)$. In particular, it follows $\mathfrak{G}(B_i, A; B) = B_i|\mathfrak{G}(A^*, A; B)$ for every $A^* \in \mathfrak{R}^{\circ}_{1.f}/B_1$ (Lemma 6.4 (b)), and

hence $B_2|\mathcal{G}(B_1, A; B) = B_2|(B_1|\mathcal{G}(A^*, A; B)) = \mathcal{G}(B_2, A; B)$.

(b) By Th. 6.3, A' contains a subring B' such that $B'[F']$ is in $\mathcal{R}_{l.f}$ for every finite subset F' of A'. If σ' is in $\mathcal{G}(A', A; B)$ then, again by Th. 6.3, $A'\sigma'$ contains a subring $B'' \in \mathcal{R}_{l.f}/(B'[B_2])\sigma'$. Obviously, $B''\sigma'^{-1}$ is in $\mathcal{R}_{l.f}/B_2$ and $B''\sigma'^{-1}|\sigma'$ is contained in $\mathcal{G}(B''\sigma'^{-1}, A; B)$. Now, our assertion is clear by (a) and its proof.

(c) Let h and v be arbitrary elements of $A' \cap H$ and of V, respectively. By Th. 6.3, A' contains some $B' \in \mathcal{R}_{l.f}/B[h]$. Since $B'\sigma'$ is in $\mathcal{R}_{l.f}$ by (b), if B'' is in $\mathcal{R}_{l.f}/(B'\sigma')[v]$ then $B'\sigma'|\sigma'^{-1} = B'\sigma'|\tau$ for some $\tau \in \mathcal{G}(B'', A; B)$ by (a). As $v\tau$ is contained in V, we have $h \cdot v\tau = v\tau \cdot h$, whence it follows $h\sigma' \cdot v = v \cdot h\sigma'$. We see therefore $h\sigma' \in H$. Now, let $h' = a'\sigma'$ $(a' \in A')$ be an arbitrary element of $A'\sigma' \cap H$. By Th. 6.3 and (b), A' contains some $B^* \in \mathcal{R}_{l.f}/B[a']$ and $\sigma^* = B^*|\sigma'$ is in $\mathcal{G}(B^*, A; B)$. If a' is not in H then there exists some $v' \in V$ such that $a'v' \neq v'a'$. Taking an arbitrary $B^{**} \in \mathcal{R}_{l.f}/B^*[v']$, by (a) we can find some $\sigma^{**} \in \mathcal{G}(B^{**}, A; B)$ such that $\sigma^* = B^*|\sigma^{**}$. Then, $v'\sigma^{**}$ is in V and $h' \cdot v'\sigma^{**} = a'\sigma^{**} \cdot v'\sigma^{**} \neq v'\sigma^{**} \cdot a'\sigma^{**} = v'\sigma^{**} \cdot h'$, which is a contradiction. We have thus $A'\sigma' \cap H \subset (A' \cap H)\sigma'$, namely, $A'\sigma' \cap H = (A' \cap H)\sigma'$.

Corollary 6.6. *Assume that* A *is w-q-Galois and left locally finite over* B. *Let* $B' \in \mathcal{R}_{l.f}$, $\sigma \in \mathcal{G}(B', A; B)$, *and* $\mathcal{H}$ *a subset of* $\mathcal{G}(B', A; B)$.

(a) σA_R *is homogeneously* B'_R-A_R-*completely reducible and the length of the composition series is equal to* $|V_A(B')|$.

(b) *If* σA_R *is* B'_R-A_R-*isomorphic to* τA_R $(\tau \in \mathcal{G}(B', A; B))$ *then* $\sigma = \tau\tilde{v}$ *with some* $v \in V'$, *and conversely*.

(c) *If* σA_R *is contained in* $\mathcal{H} A_R$ *then* $\sigma = \tau\tilde{v}$ *for some* $\tau \in \mathcal{H}$ *and* $v \in V'$.

Proof. (a) By Ths. 6.1 (b) and 6.5 (b), A is homogeneously $B'\sigma$-A-completely reducible and $[A|(B'\sigma)_L \cdot A_R] = |V_A(B'\sigma)| = |V_A(B')|$,

whence it follows our assertion.

(b) If $\tau \longleftrightarrow \sigma v_R$ $(v \in A)$ under the B'_R-A_R-isomorphism ${}_\tau A_R \cong {}_\sigma A_R$, then for every $b' \in B'$ we have $b'_R\tau \longleftrightarrow b'_R\sigma v_R = \sigma(b'\sigma \cdot v)_R$ and $\tau(b'\tau)_R \longleftrightarrow \sigma(v \cdot b'\tau)_R$, whence it follows $b'\sigma \cdot v = v \cdot b'\tau$. In particular, if b' is in B then $b'v = vb'$, which proves v is in V^*. Hence, $\sigma = \tau\,\tilde{v}$. The converse is obvious.

(c) By (a), ${}_\sigma A_R$ is B'_R-A_R-isomorphic to some ${}_\tau A_R$ $(\tau \in \mathfrak{G})$. Hence, our conclusion is given by (b).

Corollary 6.7. *Assume that A is w-q-Galois and left locally finite over B. Let B' be an intermediate ring of A/B left finite over B, and ρ a B-ring homomorphism of B' into A. If A is $B'\rho$-A-irreducible then A is B'-A-irreducible, and conversely.*

Proof. By Th. 6.5, $T_2 | \mathfrak{J}(T_1, A; B) = \mathfrak{J}(T_2, A; B)$ for every $T_1 > T_2$ in $\mathfrak{R}^{\circ}_{l.f}$. If A_o is an arbitrary member of $\mathfrak{R}^{\circ}_{l.f}/B'$ then $\rho = B'|\tau$ with some $\tau \in \mathfrak{J}(A_o, A; B)$ (Lemma 6.4 (a)). Accordingly, A is B'-A-irreducible by Prop. 5.1 (b). (Note that $B' = (B'\rho)\tau^{-1}$.) Conversely, assume that A is B'-A'irreducible. Then B' is in $\mathfrak{R}_{l.f}$ (Prop. 3.8 (a)), and so ρ is an isomorphism. Hence, our assertion is clear by the first part.

Lemma 6.8. *Let B be a simple ring, and B' in $\mathfrak{R}_{l.f}$. If $\mathrm{Hom}({}_B B', {}_B A) = \mathfrak{J}(B', A; B)A_R$ then $J(\mathfrak{J}(B', A; B)) = B$.*

Proof. If t is in $J(\mathfrak{J}(B', A; B)) \setminus B$ then $B^* = B[t]$ is a subring of B' properly containing B. Since $\mathrm{Hom}({}_B B^*, {}_B A) = B^*|\mathrm{Hom}({}_B B', {}_B A) = (B^*|\mathfrak{J}(B', A; B))A_R = (B^*|1)A_R$, it follows a contradiction $[B^*:B]_L = 1$.

We can prove now the following important theorem.

Theorem 6.9. *Let A/B be w-q-Galois and left locally finite. If B' is in $\mathfrak{R}_{l.f}$ then there holds the following:*

(a) $\mathrm{Hom}({}_{B'}B'', {}_{B'}A) = \mathfrak{J}(B'', A; B')A_R$ *for every* $B'' \in \mathfrak{R}_{l.f}/B'$.

(b) $J(\mathfrak{J}(B'', A; B')) = B'$ *for every* $B'' \in \mathfrak{R}_{l.f}/B'$.

Proof. (a) Let T be an arbitrary member of $\mathfrak{R}^{\circ}_{l.f}/B'$. Evidently, $\mathrm{Hom}({}_{B'}T, {}_{B'}A)$ is a T_R-A_R-submodule of $\mathrm{Hom}({}_B T, {}_B A) = \mathfrak{J}(T, A; B)A_R$,

and then $\mathrm{Hom}({}_B T, {}_B A) = \oplus \sum_1^s \sigma_i u_{iL} A_R$ with some $\sigma_i \in \mathcal{G}(T, A; B)$ and non-zero $u_i \in V$ (Prop. 5.7 (a), (c)). By Th. 6.1, there exists some T' in $\mathfrak{R}^{\circ}_{l.f}/T$ such that every intermediate ring A' of A/T' is homogeneously B'-A'-completely reducible with $[A'|B'_L \cdot A'_R] = |V_A(B')|$ and $\mathrm{Hom}({}_B T, {}_B A') = \mathcal{G}(T, A'; B)A'_R$. Now, let σu_L be an arbitrary $\sigma_i u_{iL}$. By Th. 6.5, there exists some $\sigma^* \in \mathcal{G}(T', A; B)$ such that $\sigma = T|\sigma^*$. If $A'' = (T'\sigma^*)[T', u]$ $(\in \mathfrak{R}^{\circ}_{l.f}/T')$, then $\sigma^{*-1} = T'\sigma^*|\tau''$ with some $\tau'' \in \mathcal{G}(A'', A; B)$ again by Th. 6.5. We set here $A' = A''\tau''$ $(\in \mathfrak{R}^{\circ}_{l.f}/T')$ and $\sigma' = \tau''^{-1}$. Let M_o be a minimal B'-A'-submodule of A' such that $N_o = M_o\sigma' u_L$ is non-zero (and so B'-A''-irreducible). Obviously, $A' = M_o \oplus M_1 \oplus \ldots \oplus M_t$ and $A'' = N_o \oplus N_1 \oplus \ldots \oplus N_t$ with some B'-A'-isomorphic M_i's and B'-A''-isomorphic N_i's, where $t + 1 = |V_A(B')|$. Then, we can easily find a B'-isomorphism ν of A' onto A'' such that $a'_R\nu = \nu(a'\sigma')_R$ for every $a' \in A'$. As $\nu^{-1}\sigma' u_L$ is contained in $\mathrm{Hom}({}_{B'}A''_{A''}, {}_{B'}A''_{A''}) = (V_{A''}(B'))_L$ (simple), $\sigma' u_L = \nu v_{1L} + \ldots + \nu v_{mL}$ with some v_j's in $V_{A''}(B')$ (Prop. 3.5). Noting that T is in $\mathfrak{R}^{\circ}_{l.f}$, one will readily see that every $(T|\nu v_{jL})A''_R$ is a T_R-A''_R-irreducible submodule of $\mathrm{Hom}({}_{B'}T, {}_{B'}A'') \subset \mathrm{Hom}({}_B T, {}_B A'') = \mathcal{G}(T, A''; B)A''_R$. It follows therefore that $(T|\nu v_{jL})A''_R = \tau w_{jL} A''_R$ with some $\tau \in \mathcal{G}(T, A''; B)$ and non-zero $w_j \in V_{A''}(B)$ (Prop. 5.7 (c)). We have then $A'' = v_j A'' = v_j \cdot (T \cdot A')\nu = v_j \cdot T\nu \cdot A'' = T(T|\nu v_{jL})A''_R = w_j \cdot T\tau \cdot A'' = w_j A''$, whence it follows that w_j is a unit of $V_{A''}(B)$. Hence, $\tau\tilde{w}_j$ is contained in $\mathcal{G}(T, A''; B) \cap \mathrm{Hom}({}_{B'}T, {}_{B'}A'')$. We have proved thus $\sigma u_L = T|\sigma' u_L$ is contained in $\mathcal{G}(T, A; B')A_R$, and so $\mathrm{Hom}({}_{B'}T, {}_{B'}A) = \mathcal{G}(T, A; B')A_R$. Our assertion is now a consequence of Lemma 6.4 (b).

(b) This follows at once from (a) and Lemma 6.8.

Corollary 6.10. Let A be left locally finite over a unital simple subring B, and $\mathfrak{H}$ a subset of $\mathcal{G}$ with $\mathfrak{H}\tilde{V} = \mathfrak{H}$.

(a) If $\mathfrak{H}A_R$ is dense in $V_{\mathcal{O}}(B_L)$ then $J(\mathfrak{H}) = B$, and $\mathcal{G}(B', A; B) = B'|\mathfrak{H}$, $\mathfrak{H}(B')A_R$ is dense in $V_{\mathcal{O}}(B'_L)$ and $J(\mathfrak{H}(B')) = B'$ for every B' in $\mathfrak{R}_{l.f}$.

(b) If $\tilde{V}A_R$ is dense in $V_{\mathfrak{o}}(B_L)$ then every simple intermediate ring B' of A/B with $[B':B]_L < \infty$ is regular and there holds $V_A^2(B') = B'$.

Proof. (a) If T is in $\mathfrak{R}^{\circ}_{l.f}$ then $\mathfrak{G}(T, A; B) \subset \mathrm{Hom}({}_BT, {}_BA) = (T \mid \mathfrak{H})A_R$ yields $\mathrm{Hom}({}_BT, {}_BA) = \mathfrak{G}(T, A; B)A_R$ and $\mathfrak{G}(T, A; B) = T|\mathfrak{H}$ (Prop. 5.7). Accordingly, for any $A' \in \mathfrak{R}^{\circ}_{l.f}/B'$ there holds $\mathfrak{G}(B', A; B) = B'|\mathfrak{G}(A', A; B) = B'|(A'|\mathfrak{H})) = B'|\mathfrak{H}$ (Th. 6.5). Now, our assertion will be easy by Lemma 6.8 and Th. 6.9.

(b) In the proof of Th. 6.1 (a) (if we set $A' = A$), $\mathfrak{G}(T^*, A; B) = T^*|\tilde{V}$ by (a), and hence $\mathfrak{m}_j = \sigma_j u_{jL} A_R = (T^*|v_{jL})A_R$ for some $v_j \in V$. Recalling that $T^*|v_{jL}$ is contained in $\mathrm{Hom}({}_{B'}T^*, {}_{B'}A)$, we see that v_j is contained in $V_A(B')$. It follows therefore $M_j = (B'e)\mathfrak{m}_j = v_j(B'eA) = v_jM$ is a B'-A-homomorphic image of M, which proves that A is homogeneously B'-A-completely reducible. Hence, $V_A(B')$ is simple. The rest of the proof is obvious by (a).

Next, we shall present the following proposition that is especially important in the study of division ring extensions.

Proposition 6.11. Let B be simple, $\mathfrak{H}$ a subgroup of $\mathfrak{G}$ containing $\tilde{V}$, and let $\mathfrak{H}A_R$ be dense in $V_{\mathfrak{o}}(B_L)$. If B' is an intermediate ring of A/B such that A is B'-A-irreducible and $[B':B]_L < \infty$ then $J(\mathfrak{H}(B')) = B'$.

Proof. We shall prove first that if $B'' = J(\mathfrak{H}(B'))$ then $\infty > [(B'|\mathfrak{H})A_R:A_R]_R = [(B''|\mathfrak{H})A_R:A_R]_R$. By Prop. 5.7, $(B'|\mathfrak{H})A_R = \oplus_1^t (B'|\sigma_i\tilde{V})A_R$ with some $\sigma_i \in \mathfrak{H}$ and there holds $\infty > [(B'|\sigma_i\tilde{V})A_R:A_R]_R = [(B'\sigma_i|\tilde{V})A_R:A_R]_R = [(B''\sigma_i|\tilde{V})A_R:A_R]_R = [(B''|\sigma_i\tilde{V})A_R:A_R]_R$, for $V_A(B'\sigma_i) = V_A(B')\sigma_i = V_A(B'')\sigma_i = V_A(B''\sigma_i)$ (cf. Prop. 5.1 (d)). Further, by Prop. 5.7 (d), $\sum_1^t (B''|\sigma_i\tilde{V})A_R = \oplus_1^t (B''|\sigma_i\tilde{V})A_R$. If τ is an arbitrary element of $\mathfrak{H}$, $B'|\tau = B'|\sigma_j\tilde{v}$ with some σ_j and $v \in V$ (Prop. 5.7 (d)). Hence, we have $B''|\tau = B''|\tau(\sigma_j\tilde{v})^{-1}(\sigma_j\tilde{v}) = B''|\sigma_j\tilde{v} \in$

$\sum_1^t (B''|\sigma_i\tilde{V})A_R$, whence it follows $[(B''|\mathfrak{H})A_R:A_R]_R = \sum_1^t [(B''|\sigma_i\tilde{V})A_R:A_R]_R$ $= \sum_1^t [(B'|\sigma_i\tilde{V})A_R:A_R]_R = [(B'|\mathfrak{H})A_R:A_R]_R$, as requested. Suppose now that $B'' \supsetneqq B'$. Then, there exists a left B-submodule M of B" properly containing B' and possessing a finite left B-basis. Since $\mathrm{Hom}({}_BM, {}_BA) = M|\mathfrak{H}A_R = M|(B''|\mathfrak{H})A_R$ by assumption, there holds $[M:B]_L = [M|(B''|\mathfrak{H})A_R:A_R]_R$. Hence, we have $[(B'|\mathfrak{H})A_R:A_R]_R = [B':B]_L < [M:B]_L \leqq [(B''|\mathfrak{H})A_R:A_R]_R$, which is a contradiction.

Corollary 6.12. *Let A and B be division rings, $\mathfrak{H}$ a subgroup of $\mathfrak{G}$ containing $\tilde{V}$, and let T be an intermediate ring of A/B left finite over B. If $J(\mathfrak{H}) = \mathfrak{B}$ then $\Gamma(T, A; B) = T|\mathfrak{H}$ and $J(\mathfrak{H}(T)) = T$.*

Proof. Since $\mathfrak{H}A_R$ is dense in $V_{\mathfrak{o}}(B_L)$ (Cor. 5.6 (b)), the assertions are evident by Props. 5.7 (d) and 6.11.

Let $A_1 > A_2$ be subrings of A. $D(A_1, A; A_2)$ will denote the set of all the derivations of A_1 into A vanishing on A_2, in particular, we write $D(A, A; A_2) = D(A; A_2)$ and $D(A_1, A; 0) = D(A_1, A)$. A regular subring T of A containing B is called an *f-regular* intermediate ring of A/B if $[V:V_A(T)]_R < \infty$. In case A/B is w-q-Galois and left locally finite, every T in $\mathfrak{L}_{l.f}$ is f-regular (Th. 6.1 (b)).

Theorem 6.13. *Let A/B be w-q-Galois and left locally finite.*

(a) *Let B' be a simple intermediate ring of A/B left finite over B. If δ is in $D(B', A; B)$ then $\delta = B'|\delta_v$ with some $v \in V$, where δ_v is the inner derivation $v_R - v_L$ effected by v.*

(b) *Let A' be an f-regular intermediate ring of A/B. If δ is in $D(A', A; B)$ then $\delta = A'|\delta_v$ for some $v \in V$.*

Proof. (a) Let e be an arbitrary primitive idempotent of B'. As $e\delta = e^2\delta$, we readily obtain $e\cdot e\delta\cdot e = 0$. If $a = [e\delta, e] = e\delta\cdot e - e\cdot e\delta$ then $[e, a] = -e\delta$. Thus, $\delta' = \delta + B'|\delta_a$ is an element of $D(B', A)$ with $e\delta' = 0$. Obviously $A = \bigoplus_\lambda B'ea_\lambda$ $(a_\lambda \in A)$, where each $a_{\lambda R}$ induces a B'-isomorphism of B'e onto $B'ea_\lambda$. Hence, by $(\sum_\lambda b'_\lambda ea_\lambda)\beta = \sum_\lambda (b'_\lambda e)\delta'\cdot a_\lambda = \sum_\lambda b'_\lambda\delta'\cdot ea_\lambda$ we can define $\beta \in \mathfrak{o}$. If $\alpha = \beta + a_L$ then for each $b' \in B'$ we have $(b'_\lambda ea_\lambda)[b'_L, \alpha] =$

$b'\delta\cdot(b'_\lambda e a_\lambda)$, whence it follows $(b'\delta)_L = [b'_L, \alpha]$. Since δ is in $D(B', A; B)$, $0 = (b\delta)_L = [b_L, \alpha]$ for every $b \in B$, namely, α is in $V_{\mathcal{C}}(B_L)$. Now, let T be an arbitrary member of $\mathfrak{R}^{\circ}_{l.f}/B'$. Then $\mathrm{Hom}({}_BT, {}_BA) = \mathfrak{J}(T, A; B)A_R = \oplus_1^s \sigma_i A_R$ ($\sigma_i \in \mathfrak{J}(T, A; B)$), and $T|\alpha$ is uniquely represented as $\sum_1^s \sigma_i x_{iR}$ with $x_i \in A$ (Prop. 5.7), where we may assume that $\sigma_i = T|\tilde{v}_i$ for $i = 1, \ldots, s'$ and $\sigma_i \notin T|\tilde{V}$ for $i = s'+1, \ldots, s$. Let b' be an arbitrary element of B'. If we define $\gamma_i \in \mathrm{Hom}(T, A)$ by $t\gamma_i = (b't)\sigma_i - b'(t\sigma_i)$ ($i = 1, \ldots, s$), then $t_R\gamma_i = \gamma_i(t\sigma_i)_R$ ($t \in T$), and it is easy to see that every $\gamma_i A_R$ is T_R-A_R-homomorphic to the irreducible module $\sigma_i A_R$. Hence, by Prop. 5.7 (d), we have $(T|1_R)(b'\delta)_L = T|(b'\delta)_L = \sum_1^s \gamma_i x_{iR} = \sum_1^{s'} \gamma_i x_{iR} = \sum_1^{s'} (T|[v_i, b']_L)y_{iR} = \sum_1^{s'} (T|y_{iR})[v_i, b']_L$, where $y_i = v_i^{-1}x_i$. Now, choose an arbitrary left $V_A(T)$-basis $\{u_\mu\}$ of A such that $u_1 = 1$, and represent y_i in terms of this basis. Then $(T|1_R)(b'\delta)_L = \sum_\mu (T|u_{\mu R})[\sum_i v_i y_{i\mu}, b']_L$. Obviously $v'_\mu = \sum_i v_i y_{i\mu}$ is an element of V determined independently on b'. It follows then $b'\delta = [v'_1, b'] = b'\delta_{-v'_1}$ by the proposition symmetric to Prop. 5.1 (d).

(b) There exists a simple intermediate ring B' of A'/B left finite over B such that $V_A(B') = V_A(A')$, and then $B'|\delta = B'|\delta_v$ for some $v \in V$ by (a). Since A/B' is w-q-Galois and locally finite (Th. 6.9), A' is an intermediate ring of $V_A^2(B')/B'$ and $\delta' = \delta - A'|\delta_v$ is contained in $D(A', A; B')$, it suffices to prove that if A' is contained in H then $\delta = 0$. To see this, we set $A' = \bigcup_\lambda B_\lambda$, where B_λ runs over all the simple intermediate rings of A'/B left finite over B. Then $B_\lambda|\delta = B_\lambda|\delta_{v_\lambda}$ with some $v_\lambda \in V$ by (a). Hence, we have $B_\lambda|\delta = 0$ for all λ, whence it follows $\delta = 0$.

Now, we shall introduce the following definitions: A/B is said to be <u>q-Galois</u> if B is regular and A/B is w-q-Galois. Symmetrically, we can define <u>right q-Galois extensions</u>. While, A/B is said to be <u>h-Galois</u> (resp. <u>right h-Galois</u>) if B is regular and $\mathfrak{J}A_R$ is dense in

in $V_{\mathfrak{o}\mathfrak{l}}(B_L)$ (resp. if $\mathfrak{G} A_L$ is dense in $V_{\mathfrak{o}\mathfrak{l}}(B_R)$).

Proposition 6.14. Assume that for every finite subset F of A there exists an intermediate ring A^* of $A/B[F]$ such that A^*/B is h-Galois. If A/B is left locally finite then A/B is q-Galois.

Proof. Let T be in $\mathfrak{R}^{\circ}_{l.f}$, and A^* an intermediate ring of A/T such that A^*/B is h-Galois. Then $\mathrm{Hom}({}_BT, {}_BA) = \mathrm{Hom}({}_BT, {}_BA^*)A_R = ((T \mid \mathfrak{G}^*)A^*_R)A_R = \mathfrak{G}(T, A; B)A_R$, where $\mathfrak{G}^*$ is the group of B-ring automorphisms of A^*. To see that V is simple, we represent the simple ring $V_{A^*}(B)$ as the complete matrix ring over a division ring with a system of matrix units Γ^*. If $T^* = T[\Gamma^*]$ then $V_{T^*}(B)$ is a simple ring. Since $V = \bigcup_{T \in \mathfrak{R}^{\circ}_{l.f}} V_{T^*}(B)$, our assertion is a consequence of Prop. 3.7.

If $J(\mathfrak{G}) = B$, A/B is said to be w-Galois. A/B is defined to be Galois if B is regular and A/B is w-Galois. In case A/B is Galois, $\mathfrak{G}$ is called the Galois group of A/B and denoted by $\mathfrak{G}(A/B)$, and in general a subgroup $\mathfrak{H}$ of $\mathfrak{G}$ with $J(\mathfrak{H}) = B$ is called a Galois group of A/B. If A/B is h-Galois and left locally finite then A/B is Galois by Cor. 6.10. On the other hand, if A is h-Galois over a division subring B then one will easily see that A/B is Galois. Accordingly, in case A is a division ring, the notion of Galois coincides with that of h-Galois (Th. 2.5). One will see later that finite (dimensional) Galois extensions, left locally finite Galois extensions with the locally compact Galois groups and other important Galois extensions treated by now are all h-Galois, and Prop. 6.14 enables us to see that left locally finite h-Galois extensions and the related extensions (for instance, locally Galois extensions (cf. §16)) are q-Galois. In case A/B is h-Galois and left locally finite, Ths. 6.1 and 6.5 will be used often without mentioning the validity of Prop. 6.14. Finally, we shall state the following:

Proposition 6.15. Let A be w-q-Galois and left locally finite over B, and $\mathfrak{T} = V_{\mathfrak{o}\mathfrak{l}}(B_L \cdot B_R)$. If T is in $\mathfrak{R}^{\circ}_{l.f}$ then $T \mid \mathfrak{T} = \mathrm{Hom}({}_BT_B, {}_BA_B) = \mathfrak{G}(T, A; B)V_R$. In particular, $\mathfrak{T} A_R$ is dense in $V_{\mathfrak{o}\mathfrak{l}}(B_L)$.

Proof. Obviously, $T|\mathfrak{T} \subset \mathrm{Hom}({}_BT_B, {}_BA_B) = \mathcal{G}(T, A; B)V_R$ (cf. Prop. 5.7). Now, we shall prove converse inclusion. Let σ be an element of $\mathcal{G}(T, A; B)$. We consider here the family $\Phi = \{(f, M)\}$, where M is a T-T-submodule of A containing T and f is a B-B-homomorphism of M into A such that $T|f = \sigma$. Defining the usual ordering in Φ, we readily see that Φ is inductive. Let (f', M') be maximal in Φ, and suppose that $M' \neq A$. There exists then some $T' \in \mathfrak{L}^{\circ}_{l.f}/T$ such that $T' \not\subset M'$. If $M'' = M' \cap T'$ then $M''|f' = M''|g$ for some g in $\mathcal{G}(T', A; B)V_R$. To be easily seen, the well-defined map $h: m' + t' \longrightarrow m'f' + t'g$ $(m' \in M', t' \in T')$ is contained in $\mathrm{Hom}({}_B(M' + T')_B, {}_BA_B)$, which contradicts the maximality of (f', M').

Nagahara [8], [10], [11]; Nagahara-Tominaga [8], [9], [11]; Tominaga [8], [9], [10], [11].

7. Fundamental theorem of finite Galois theory

The statements in Props. 5.1 and 5.7 are especially valid for the case $B' = A$. In what follows, without mention, we shall use freely those.

Let $\mathfrak{G}$ be an automorphism group of the ring A. Obviously, $\mathfrak{G}A_R$ is A_R-A_R-completely reducible and each of its homogeneous components is of the form $\sigma\mathfrak{G}_o A_R$ where $\mathfrak{G}_o = \mathfrak{G} \cap \tilde{A}$. Let $I(\mathfrak{G})$ be the subring of A generated by all the units v of A with $\tilde{v} \in \mathfrak{G}$. We have then $\sigma\mathfrak{G}_o A_R = \sigma I(\mathfrak{G})_L \cdot A_R$, and hence $[\sigma\mathfrak{G}_o A_R : A_R]_R = [I(\mathfrak{G}):C]$. It follows therefore $[\mathfrak{G}A_R : A_R]_R = (\mathfrak{G} : \mathfrak{G}_o)\cdot[I(\mathfrak{G}):C]$, that will be called the <u>reduced order</u> of $\mathfrak{G}$. Now, assume that $B = J(\mathfrak{G})$ is simple and $[A:B]_L < \infty$. Then, we have $\infty > [A:B]_L = [V_{\mathfrak{o}}(B_L):A_R]_R \geqslant [\mathfrak{G}A_R : A_R]_R = (\mathfrak{G} : \mathfrak{G}_o)\cdot[I(\mathfrak{G}):C]$. Next, assume $I(\mathfrak{G})$ is two-sided simple. Since an arbitrary A_R-A_R-irreducible submodule of $\mathfrak{G}A_R$ is $\sigma u_L A_R$ with some $\sigma \in \mathfrak{G}$ and non-zero $u \in A$ and isomorphic to σA_R, we have $\sigma u_L A_R \subset \sigma\mathfrak{G}_o A_R = \sigma I(\mathfrak{G})_L \cdot A_R$, whence it follows that u_L is contained in $V_{I(\mathfrak{G})_L \cdot A_R}(A_R) = I(\mathfrak{G})_L$. The last fact enables us to see that $\mathfrak{G}A_R$ is two-sided simple. We assume here additionally that the reduced order of $\mathfrak{G}$ is finite. Then $I(\mathfrak{G})$ and $\mathfrak{G}A_R$ are evidently simple, and Th. 3.11 proves that $B_L = V_{\mathfrak{o}}(\mathfrak{G}A_R)$ is simple and $\mathfrak{G}A_R = V^2_{\mathfrak{o}}(\mathfrak{G}A_R) = V_{\mathfrak{o}}(B_L)$. Hence, we have $[A:B]_L = [\mathfrak{G}A_R : A_R]_R < \infty$. Moreover, we obtain $V_L = A_L \cap V_{\mathfrak{o}}(B_L) = A_L \cap \mathfrak{G}A_R = I(\mathfrak{G})_L$, namely, $V = I(\mathfrak{G})$.

An automorphism group $\mathfrak{G}$ of the ring A is called an <u>N*-group</u> if $I(\mathfrak{G})$ is simple, and an N*-group of finite reduced order is called an <u>N-group</u>. Every finite N*-group $\mathfrak{G}$ is evidently an N-group and there holds $[A:B] \leqslant \#\mathfrak{G}$ for $B = J(\mathfrak{G})$, and will be called an <u>F-group</u>. If $I(\mathfrak{G})$ is a division ring and $\mathfrak{G}$ is of finite order, then $\mathfrak{G}$ is called a <u>DF-group</u>. In case A is a division ring, every finite automorphism group $\mathfrak{G}$ of A is a DF-group. If $\mathfrak{G}$ is an N*-group (resp. N-group) and $I(\mathfrak{G})^{\sim} \subset \mathfrak{G}$ then $\mathfrak{G}$ is called an <u>N*-regular group</u> (resp. <u>N-regular group</u>). We shall define here $V(\mathfrak{G})$

as the subring $V_A(J(\mathfrak{H}))$. If $V(\mathfrak{H})$ is simple and $V(\mathfrak{H})^{\sim} \subset \mathfrak{H}$ then $\mathfrak{H}$ is called a (*)-regular group, and a (*)-regular group $\mathfrak{H}$ with simple $J(\mathfrak{H})$ is called a regular group. Obviously, every (*)-regular group is N*-regular, in particular, if A is finite Galois over B then $\mathfrak{G}(A/B)$ is N-regular. Conversely, assume that $\mathfrak{H}$ be N-regular and $B = J(\mathfrak{H})$. Then $V_{\mathfrak{R}}(B_L) = \mathfrak{H}A_R$ (and so A/B is h-Galois) and $\tilde{V} = I(\mathfrak{H})^{\sim} \subset \mathfrak{H}$, and hence $\mathfrak{H}$ coincides with $\mathfrak{G}(A/B)$ (Prop. 5.7). Summarizing the above, we obtain the following:

Proposition 7.1. (a) If $\mathfrak{H}$ is an N-group of A then $B = J(\mathfrak{H})$ and H are simple, $V = I(\mathfrak{H})$, $[A:B] = (\mathfrak{H} : \mathfrak{H}_0)\cdot[I(\mathfrak{H}):C] < \infty$ and $V_{\mathfrak{R}}(B_L) = \mathfrak{H}A_R$, and hence A/B is finite Galois.

(b) Let A be Galois and left finite over B with a Galois group $\mathfrak{H}$. Then $[A:B]_R = [A:B]_L$, and the following conditions are equivalent: (1) $\mathfrak{H}$ is an N*-group, (2) $\mathfrak{H}$ is an N-group, and (3) $V_{\mathfrak{R}}(B_L) = \mathfrak{H}A_R$. If $\mathfrak{H}$ is N-regular then $\mathfrak{H}$ coincides with $\mathfrak{G}$.

Combining Prop. 7.1 with Cor. 6.10, we obtain the following at once.

Theorem 7.2. Let A be finite Galois over B.

(a) There exists a 1-1 dual correspondence between regular intermediate rings of A/B and N*-regular (or (*)-regular) subgroups of $\mathfrak{G}$, in the usual sense of Galois theory.

(b) Every B-ring isomorphism between regular intermediate rings of A/B can be extended to an element of $\mathfrak{G}$.

In case A/B is an infinite Galois extension, as will be shown in §22, there exists some difference between N*-regular groups and (*)-regular groups, and the fundamental theorem for the case of infinite dimension will be concerned with (*)-regular groups.

By the validity of Prop. 7.1, the first assertion of the next is a consequence of Prop. 3.8 and Th. 6.1 (b), and the second is contained in Cor. 6.2.

Proposition 7.3. Let A be finite Galois over B.

(a) Let T be an intermediate ring of A/B. If A is T-A-irreducible then T is a simple ring such that $V_A(T)$ is a division ring, and conversely.

(b) If V is a division ring then every intermediate ring of A/B is simple, and conversely.

Concerning the outer case, Props. 7.1, 7.3 and Th. 7.2 prove the following, that may be stated without proof.

Theorem 7.4. Let $\mathfrak{H}$ be a finite outer automorphism group of A such that $B = J(\mathfrak{H})$ (or let A be finite Galois over B with an outer Galois group $\mathfrak{H}$). Then, every intermediate ring of A/B is simple, $[A:B] = \#\mathfrak{H} = \#\mathfrak{G}$, $V = C$, and there exists a 1-1 dual correspondence between intermediate rings of A/B and subgroups of $\mathfrak{G}$, in the usual sense of Galois theory.

Corollary 7.5. Let A be left locally finite over a simple subring B, and $\mathfrak{G}'$ a subgroup of $\mathfrak{G}$ with $A' = J(\mathfrak{G}')$. If $[A':B]_L < \infty$ and $V_A(A') = C$ then A' is a simple ring.

Proof. If $B' = A'[E]$, then $(B'|\mathfrak{G}')A_R = \oplus_1^m (B'|\sigma_i)A_R$ with some $\sigma_i \in \mathfrak{G}'$ (Prop. 5.7). Noting that $V_A(A') = C$, one will readily see that $B'|\mathfrak{G}' = \{B'|\sigma_1, \cdots, B'|\sigma_m\}$ (Prop. 5.7). Obviously, $B_o = B'[\cup_i B'\sigma_i]$ is a $\mathfrak{G}'$-invariant simple subring of A and $B_o|\mathfrak{G}'$ is an automorphism group of finite order. Hence, $A' = J(B_o|\mathfrak{G}')$ is simple by Th. 7.4.

Let A be Galois over B. The case that $\mathfrak{G}$ contains no inner automorphisms except the identity, namely, the case $V = C$, and the case that $J(\tilde{V}) = B$ are the extremes. We say that A/B is outer Galois or inner Galois according as it happens the first case or the second case. By Cor. 4.9, every outer Galois extension over a field is commutative. If A/B is finite Galois then A/H and H/B are respectively inner Galois and outer Galois (cf. Prop. 3.5) and one will readily see that $[A:H] = [V:C]$ and $[H:B] = (\mathfrak{G}:\tilde{V})$ (Prop. 7.1). We shall present here a partial converse of Th. 7.4.

Proposition 7.6. Let A be finite Galois over B. If [A:B] coincides with the order of $\mathfrak{G}$ then A/B is outer Galois.

Proof. Since $(\mathfrak{G}:\tilde{V}) = [H:B]$, we obtain $\#\tilde{V} = [A:H]$. Thus, to our end, it suffices to prove that if A is inner Galois and finite

over B and $\#\tilde{V} = [A:B] = [V:C] = g$ then $g = 1$. As $\#\tilde{V} < \infty$, either $V = C$ or $\#V < \infty$ by Prop. 3.10. Hence, in what follows, we may restrict our attention to the case $\#V < \infty$. Let $V = \sum_1^r Ug_{pq}$, and choose an arbitrary basis $\{u_1, \ldots, u_s\}$ of U over $C = GF(t)$. Suppose first that $r > 1$. Then, the following set X contained in V^* defines $s(r^2 + 1)$ $(> g)$ different inner automorphisms: $X = \{u_i\ (i = 1, \ldots, s), u_i(1 + g_{pq})\ (i = 1, \ldots, s;\ p \neq q), u_i(1 + g_{p1})(1 + g_{1p})\ (i = 1, \ldots, s;\ p \neq 1), u_i \sum_p g_{pr-p+1}\ (i = 1, \ldots, s)\}$. This contradiction means $r = 1$, namely, $g = s$. Suppose next $g > 1$. Then $\#\tilde{V} = (U^*:C^*) = (t^g - 1)/(t - 1) > g$, which is a contradiction.

Concerning the inner Galois case, we obtain the following that is known as the fundamental theorem of simple rings.

Theorem 7.7. *If I is a simple intermediate ring of A/C with $[I:C] < \infty$, and $B = V_A(I)$, then A/B is inner Galois, $V = I$, $[A:B] = [I:C]$, $\mathfrak{G} = \tilde{I}$, and $I' \longrightarrow V_A(I')$ and $B' \longrightarrow V_A(B')$ are mutually converse 1-1 dual correspondences between simple intermediate rings I' of I/C and simple intermediate rings B' of A/B.*

Proof. Since $\tilde{I}$ is an N-regular group and every simple intermediate ring of A/B is regular (Prop. 7.1 and Cor. 6.10 (b)), our theorem is clear by Prop. 7.1 and Th. 7.2.

Corollary 7.8. *Let A be Galois and finite over B. If T is in $\mathfrak{K}$ then $H[T] = V_A^2(T)$ is outer Galois over T and $\mathfrak{G}(V_A^2(T)/T) \simeq \mathfrak{G}(H/T \cap H)$ by the contraction map.*

Proof. As A/T is Galois (Th. 7.2), $V_A^2(T)/T$ is outer Galois. Hence, $H[T]$ is simple as an intermediate ring of $V_A^2(T)/T$ (Prop. 7.3). Moreover, there holds $V_A(V_A^2(T)) = V_A(H[T])$, and so we obtain $V_A^2(T) = H[T]$ by Th. 7.7. The rest of the proof is evident by Th. 7.4.

In case R is left algebraic over a unital simple subring S, R/S is said to be *of bounded degree* if $[S[x]:S]_L$ $(x \in R)$ is bounded with a fixed integer.

Corollary 7.9. *If a division ring* A *is algebraic and of bounded degree over* C *then* A *contains a separable maximal subfield* M *over* C *and* $[A:C] < \infty$.

Proof. It suffices to prove the case that A is of characteristic $p \neq 0$. Let A_0 be the set of all the elements x of A separable over C. Then there exists an $x_0 \in A_0$ such that $[C[x_0]:C] \geqslant [C[x]:C]$ for all $x \in A_0$. We shall prove then $M = C[x_0]$ is a maximal subfield of A. Suppose on the contrary $M' = V_A(M) \supsetneqq M$. Then $V_A^2(M) = M$ by Th. 7.7, and hence M coincides with the center of M'. Since every element of $M' \setminus M$ is inseparable over M, there exists an element $a \in M' \setminus M$ such that $a^p \in M$. Hence, we have $(\tilde{a} - 1)^p = \tilde{a}^p - 1 = 0$, where $\tilde{a}$ is considered in M'. Choose here an element $c \in M'$ with $ac \neq ca$, i.e. $c(\tilde{a} - 1) \neq 0$. Then, recalling that $c(\tilde{a} - 1)^p = 0$, we can find a positive integer i such that $d(\tilde{a} - 1) \neq 0$ and $d(\tilde{a} - 1)^2 = 0$ for $d = c(\tilde{a} - 1)^{i-1}$. If $b = d(d(\tilde{a} - 1))^{-1}$ then $b\tilde{a} - b = 1$. (Note that $d(\tilde{a} - 1)\tilde{a} = d(\tilde{a} - 1)$.) On the other hand, b^{p^f} is contained in M for some positive integer f, and so $b^{p^f} = b^{p^f}\tilde{a} = (b\tilde{a})^{p^f} = (b + 1)^{p^f} = b^{p^f} + 1$, which implies a contradiction $0 = 1$. We have seen thus M is a maximal subfield. Finally, $[A:C] = [A:M]\cdot[M:C] = [M:C]^2$ by Th. 7.7.

Proposition 7.10. *If* A *satisfies a standard identity then* $[A:C] < \infty$.

Proof. To our end, it suffices to prove the assertion for the case that A is a division ring satisfying the standard identity of degree m. Let M be a maximal subfield of A. If we set $S = M \otimes_C A \simeq M_L \cdot A_R$, A may be regarded as an irreducible (faithful) right S-module. Hence, S is a primitive ring with $E(A_S) = M_L$. If $[A:M]_L = \infty$ then, by the proof of Prop. 3.1, for every positive integer p we can find a subring T of S such that $(M)_p$ is a homomorphic image of T. Evidently $S = M \otimes_C A$ satisfies the standard identity of degree m, and hence so does $(M)_p$. But, this contradicts Prop. 3.13. We obtain therefore $[A:C] = [A:M]^2 < \infty$ (Th. 7.7).

Corollary 7.11. Let B be a simple subring of A. If $[A:C] < \infty$ then $[B:Z] < \infty$. Conversely, if $[A:B]_L < \infty$ and $[B:Z] < \infty$ then $[A:C] < \infty$.

Proof. As A satisfies a standard identity, the subring B does the same. Hence, $[B:Z] < \infty$ by Prop. 7.10. Conversely, if $[A:B]_L < \infty$ and $[B:Z] < \infty$ then $[A:Z]_L = p < \infty$, and so A may be regarded as a subring of the complete matrix ring $(Z)_p$ over the field Z. Since $(Z)_p$ satisfies a standard identity, $[A:C] < \infty$ again by Prop. 7.10.

As an application of Cor. 7.11, we obtain the following:

Proposition 7.12. Let B be a simple subring of A with $[B:Z] < \infty$.

(a) If $[A:B]_L < \infty$ then $[A:B]_R < \infty$. Accordingly, if A/B is left locally finite then it is (two-sided) locally finite.

(b) If B is a regular subring of A then $[A:B]_L = [A:B]_R$ provided we do not distinguish between two infinite dimensions.

Proof. (a) Cor. 7.11 proves $A = \sum_1^s a_i C$. Since $C \cdot B = \sum_1^t Bc_j$ ($c_j \in C$), it follows $\sum_{i,j} a_i c_j B = \sum_i a_i C \cdot B = A$, which means $[A:B]_R < \infty$.

(b) Assume $[A:B]_L < \infty$. Since $B \cdot V = B \otimes_Z V$ is a simple intermediate ring of A/C and $[A:C] < \infty$ (Cor. 7.11), we obtain $[A:B \cdot V] = [C_o:C]$ (Th. 7.7) and $[B \cdot V:B] = [V:Z]$. Hence, $[A:B]_L = [A:B]_R$.

Now, let A be a left quadratic extension of a simple subring B: $A = B \oplus Ba$. If x is in $A \setminus B$, then $BxA + B$ is a subring of A properly containing B, and $BxA + B = A$. Hence, there exists an element $b \in B$ such that $a - b \in BxA$. Noting that $A = B + B(a - b)$, we obtain $A(B(a - b)A) = (B + B(a - b))(B(a - b)A) \subset B(a - b)A$, and hence $A = B(a - b)A = BxA$. We have seen therefore that A is B-A-irreducible. Accordingly, V is a field such that $[V:C] \leqq [A:B]_L = 2$ (Prop. 5.4 (b)). Now, we shall prove the following:

Theorem 7.13. Let A be a left quadratic extension of a simple ring B. If B is finite over Z and not of characteristic 2 then

A/B is Galois.

Proof. A is inner Galois and finite over C (Cor. 7.11). If $V \neq C$ or $B \supset C$, A/B is inner Galois (Th. 7.7). Hence, in what follows, we assume $V = C$ and $B \not\supset C$. To be easily seen, there exists an element $c \in C \backslash B$ such that $c^2 \in B$. Now, one will see that the mapping $\sigma : x + yc \longrightarrow x - yc$ $(x, y \in B)$ is an automorphism of A and $J(\sigma) = B$.

Theorem 7.14. Let A be finite Galois over B, T in $\mathfrak{R}$, $\mathfrak{H}$ the group of all B-ring automorphisms of T, $\mathfrak{T} = \{\sigma \in \mathfrak{G} ; T\sigma = T\}$ and $\mathfrak{T}^* = \mathfrak{T} \cdot V(\mathfrak{T})^{\sim}$. In order that $J(\mathfrak{H}) = B$ it is necessary and sufficient that $\mathfrak{T}^* = \mathfrak{G}$.

Proof. By Th. 7.2, $J(\mathfrak{G}(T)) = T$, $T|\mathfrak{T} = \mathfrak{H}$ and $\mathfrak{G}(T) \subset \mathfrak{T}$. If $J(\mathfrak{H}) = B$ then $J(\mathfrak{T}) = J(\mathfrak{H}) = B$, and hence $\mathfrak{T}^* = \mathfrak{T} \cdot \widetilde{V} =$ (Th. 7.2). The converse will be evident.

Corollary 7.15. Let A be outer Galois and finite over B. In order that an intermediate ring T of A/B be Galois over B, it is necessary and sufficient that T be $\mathfrak{G}$-invariant: $T\mathfrak{G} = T$.

Proof. By Prop. 7.3 (b), T is in $\mathfrak{R}$. If T/B is Galois then $\mathfrak{T} = \{\sigma \in \mathfrak{G} ; T\sigma = T\} = \mathfrak{G}$ (Th. 7.14), whence T is $\mathfrak{G}$-invariant. Concerning the converse, there is nothing to prove.

Corresponding to Cor. 7.15, we can prove the next that is stated without proof. (Cf. the proof of Cor. 21.7.)

Proposition 7.16. Let A be inner Galois and finite over B, and B' a simple intermediate ring of A/B. If B'/B is inner Galois then the center Z' of B' is contained in Z, and conversely.

Azumaya [2]; Bourbaki [2]; Cartan [1], [2], [3]; Dieudonné [1]; Hattori [1]; Hochschild [1]; Jacobson [2], [6]; Moriya [1], Nagahara-Onodera-Tominaga [1]; Nakayama [3], [4], [5], [7], [8]; Rosenberg-Zelinsky [1]; Tominaga [1], [12].

8. Preliminary computation with matrix units

The present section is exclusively devoted to giving several preliminary propositions which will be needed in §§ 9-12 and § 21, and whose proofs will be accomplished by somewhat complitated computations with matrix units. Throughout the present section, A is assumed to be a simple ring with the capacity $n > 1$, and B a unital simple subring of A.

Lemma 8.1. If $e_{ii}A \cap B \neq 0$ for every $i = 1, \ldots, n$ then $e_{11}, \ldots, e_{nn}$ are all contained in B.

Proof. Since $\mathfrak{A}_i = e_{ii}A \cap B$ is a non-zero right ideals of B and $|B| \leqslant n$, we obtain $B = \mathfrak{A}_1 \oplus \ldots \oplus \mathfrak{A}_n$. Hence $e_{11} + \ldots + e_{nn} = 1 = b_1 + \ldots + b_n$ with some $b_i \in \mathfrak{A}_i \subset e_{ii}A$, whence it follows $e_{ii} = b_i \in B$.

Proposition 8.2. Let T be a simple intermediate ring of A/B left algebraic over B.

(a) Let (x_{ij}) be an element of $(D)_n$ with $x_{1n} \neq 0$ and $x_{i1} = 0$ for every $i > 1$. If T contains the elements $a = \sum x_{ij}e_{ij}$ and $u = \sum_2^n e_{ii-1}$ then T contains E and x_{ij}'s.

(b) Let $x \neq 0$, y, d and d' be elements of D. If $n = 2$ and T contains the elements $a = de_{11} + d'e_{21} + e_{12}$ and $v = xe_{21} + ye_{22}$ then T contains E, x, y, d and d'.

Proof. (a) Evidently, $u^{k-1}au^{n-1} = x_{1n}e_{k1}$ is a non-zero element of $e_{kk}A \cap T$ $(k = 1, 2, \ldots, n)$. Hence T contains all e_{ii}'s (Lemma 8.1), and so $x_{1n}e_{1n} = e_{11}ae_{nn} \in T$ and $x_{1n} = (u + x_{1n}e_{1n})^n \in T$. It follows therefore $e_{1n} = x_{1n}^{-1}(x_{1n}e_{1n}) \in T$, and then $e_{ij} = u^{i-1}e_{1n}u^{n-j}$ and $x_{ij} = \sum_k e_{ki}ae_{jk}$ are in T.

(b) $av = xe_{11} + ye_{12}$ and v are non-zero elements of $e_{11}A \cap T$ and of $e_{22}A \cap T$, respectively. Hence T contains e_{11} and e_{22} (Lemma 8.1), and so $e_{12} = e_{11}ae_{22}$ and $xe_{21} = e_{22}ve_{11}$ are contained in T. It follows then $x = (e_{12} + xe_{21})^2 \in T$ and $e_{21} = x^{-1}(xe_{21}) \in T$.

Proposition 8.3. *Let* $x \neq 0$ *and* y *be elements of* D, *and* $a = \sum d_{ij}e_{ij}$ $(d_{ij} \in D)$ *an element of* A *not contained in* C.

(a) *There exists an element* $r \in A^{\cdot}$ *such that* $a\tilde{r} = \sum x_{ij}e_{ij}$ $(x_{ij} \in D)$ *with* $x_{1n} = x$ *and* $x_{in} = 0$ *for every* $i > 1$.

(b) *If* $n > 2$ *then there exists an element* $r \in A^{\cdot}$ *such that* $a\tilde{r} = \sum x_{ij}e_{ij}$ $(x_{ij} \in D)$ *with* $x_{1n} = x$, $x_{1n-1} = y$ *and* $x_{in} = 0$ *for every* $i > 1$.

Proof. If a is diagonal then either there exist distinct suffices h, k with $d_{hh} \neq d_{kk}$ or a is an element of D not contained in C. In the first case, we obtain $a\tilde{t} = a + (d_{kk} - d_{hh})e_{hk}$ for $t = 1 + e_{hk}$. While, in the second case, there exists an element $d \in D$ with $da \neq ad$ and $a\tilde{t} = a + (da - ad)e_{12}$ for $t = 1 + de_{12}$. We may assume thus, from the beginning, that a is non-diagonal. If $\begin{pmatrix} i \\ p_i \end{pmatrix}$ is an arbitrary permutation of $1, 2, \ldots, n$, then the mapping $\pi : \sum y_{ij}e_{p_ip_j} \longrightarrow \sum y_{ij}e_{ij}$ $(y_{ij} \in D)$ is a D-ring automorphism of A. As A is inner Galois and finite over D, π is an inner automorphism effected by a unit of $\sum Ce_{ij}$ (Th. 7.7). Accordingly, without loss of generality, we may assume further that $d_{1n} \neq 0$. Under this situation, if $t = (\sum_{1}^{n-1} e_{ii} + d_{1n}e_{nn})(1 - d_{nn}d_{1n}^{-1}e_{n1}) \cdots (1 - d_{2n}d_{1n}^{-1}e_{21})$ then $a^* = a\tilde{t} = \sum d_{ij}^*e_{ij}$ $(d_{ij}^* \in D)$ with $d_{1n}^* = 1$ and $d_{in}^* = 0$ for every $i > 1$. If $s = \sum_{1}^{n-1} e_{ii} + x^{-1}e_{nn}$ then $a^*\tilde{s} = \sum x_{ij}e_{ij}$ with $x_{1n} = x$ and $x_{in} = 0$ for every $i > 1$, proving (a). To see (b), choose an element $y' \in D$ such that $d_{1n-1}^* + y' = y$. Then, for $s' = s(1 - y'e_{nn-1})$ we obtain $a^*\tilde{s'} = \sum x_{ij}e_{ij}$ with $x_{1n} = x$, $x_{1n-1} = y$ and $x_{in} = 0$ for every $i > 1$.

Lemma 8.4. *Let* T *be a subring of* A.

(a) *If* T *contains* $a = \sum x_{ij}e_{ij}$ $(x_{ij} \in D)$ *with* $x_{1n} \neq 0$ *and* $u = \sum_{2}^{n} x_ie_{ii-1}$ *with non-zero* x_i*'s in* D *then* A *is* T-A-*irreducible*.

(b) Let T be unital and left Artinian. If T contains $a = \sum x_{ij}e_{ij}$ $(x_{ij} \in D)$ with $x_{1n} = 1$ and $x_{in} = 0$ for every $i > 1$ and $u(E, d) = de_{21} + \sum_{3}^{n} e_{ii-1}$ with non-zero d in D, then T contains E, d and x_{ij}'s.

Proof. (a) Let M be an arbitrary non-zero T-A-submodule of A. Then M contains an element $a_o = \sum_{p}^{n} d_i e_{in}$ with $d_p \neq 0$. Since $u^{n-p}a_o = x_n \cdots x_{p+1} d_p e_{nn}$ belongs to M, e_{nn} is in M, whence it follows that M contains $u^{n-k} \sum_{i} x_{in}e_{in} = \sum_{2}^{k} x_{n-k+i} \cdots x_{i+1}x_{in}e_{n-k+in} + x_{n-k+1} \cdots x_2 x_{1n} e_{n-k+1n}$ $(k = 1, 2, \ldots, n)$. Recalling that $x_{1n} \neq 0$, one will see inductively that $e_{nn}, e_{n-1n}, \cdots, e_{1n}$ are in M. Accordingly, every e_{ij} is contained in M, whence we obtain M = A.

(b) By (a) and Prop. 3.8 (a), T is a simple ring. We set $u = u(E, d)$. Since $u^{k-1}au^{n-1} = d^2 e_{k1}$ is a non-zero element of $T \cap e_{kk}A$, T contains $e_{11}, e_{22}, \cdots, e_{nn}$ (Lemma 8.1). It follows therefore $e_{1n} = e_{11}ae_{nn} \in T$ and $d = (u + e_{1n})^n \in T$. Hence, we have $e_{21} = d^{-2}(d^2 e_{21}) \in T$ and $\sum_{2}^{n} e_{ii-1} = (1 - d)e_{21} + u \in T$. Now, our assertion is a consequence of Prop. 8.2 (a).

Corollary 8.5. If A is left algebraic (resp. left algebraic and of bounded degree) over B, then there exists some $B' = \sum_{1}^{n} D'e'_{ij}$ $\mathfrak{R}^{\circ}_{1.f}$ such that $V_A(\{e'_{ij}\})/D'$ is left algebraic (resp. left algebraic and of bounded degree).

Proof. In case B is contained in C, there is nothing to prove. Henceforth, we assume $B \not\subset C$. By Lemma 8.3 (a), there exists an element $r \in A^{\cdot}$ such that $B\tilde{r}$ contains an element $a = \sum x_{ij}e_{ij}$ with $x_{1n} = 1$ and $x_{in} = 0$ for every $i > 1$. Given a non-zero element $d \in D$, we set $u = u(E, d)$. Then, $(B\tilde{r})[u]$ is left finite over $B\tilde{r}$ and contains E and d (Lemma 8.4 (b)). If we set $B^* = (B\tilde{r})[E] = \sum D^*e_{ij}$ with the division ring $D^* = V_{B^*}(E)$, then D/D^* is left algebraic. Hence, $B^*\tilde{r}^{-1}$ can be taken as B' requested.

Lemma 8.6. Let A be of finite rank over a subfield Φ of C, $n = 2$, and $f(\lambda) = \lambda^2 - c\lambda - c'$ a polynomial in $C[\lambda]$. If x and y are non-zero elements of D with $f(y^{-1}x) \neq 0$ then $\Phi[a, v] \cap De_{21} \neq 0$, where $a = ce_{11} + c'e_{21} + e_{12}$ and $v = xe_{21} + ye_{22}$.

Proof. To be easily seen, $va = (xc + yc')e_{21} + xe_{22}$ and $(va)^2 = (x^2c + xyc')e_{21} + x^2e_{22}$. Now, let $g(\lambda) = \sum_0^m c_i\lambda^i \in \Phi[\lambda]$ be a minimal polynomial of y with $c_0 = 1$ and $c_m \neq 0$. As $v^i = y^{i-1}xe_{21} + y^ie_{22}$ $(i \geqslant 1)$, we obtain $g(v) = e_{11} + \sum_1^m c_iy^{i-1}xe_{21} + \sum_0^m c_iy^ie_{22} = e_{11} - y^{-1}xe_{21}$, and then one will easily verify that $(va)^2g(v) = \{(x^2c + xyc')e_{21} + x^2e_{22}\}\cdot(e_{11} - y^{-1}xe_{21}) = -xy\{(y^{-1}x)^2 - c(y^{-1}x) - c'\}e_{21}$.

Proposition 8.7. Let A be of finite rank over a subfield Φ of C, and B an intermediate ring of A/Φ. Let $A^* = \sum_1^{n^*} D^*e^*_{ij}$ ($E^* = \{e^*_{ij}\}$ a system of matrix units and $D^* = V_{A^*}(E^*)$ a division ring) be a simple intermediate ring of A/B with the center C^*, and $Z\cdot C^* = Z[c_0]$ for some $c_0 \in A^* \cap C$.

(a) Assume that $n^* \geqslant 2$ and $a = \sum x_{ij}e^*_{ij}$ $(x_{ij} \in D^*)$ is an element of A^* with $x_{1n^*} \neq 0$ and $x_{in^*} = 0$ for every $i > 1$. If c_0 is contained in $Z[\{x_{ij}\}]$ and $D^* = C^*[\{x_{ij}\}]$ then there exists a unit a' of A^* such that $A^* = Z[a, a']$.

(b) Assume that $n^* = 2$ and $a = de^*_{11} + d'e^*_{21} + e^*_{12}$ is an element of A^* $(d, d' \in D^*)$. If there exists a non-zero element $y \in D^*$ such that $Z[y] \ni c_0$ and $D^* = C^*[y, d, d']$ then $A^* = Z[a, ye^*_{21}]$.

(c) Assume that $n^* = 2$ and $a = ce^*_{11} + c'e^*_{21} + e^*_{12}$ is an element of A^* with $c, c' \in C^*$. If there exist non-zero elements $x, y \in D^*$ such that $Z[y] \ni c_0$, $D^* = C^*[x, y]$ and $(y^{-1}x)^2 - c(y^{-1}x) - c' \neq 0$ then $A^* = Z[a, xe^*_{21} + ye^*_{22}]$.

Proof. (a) Set $u^* = \sum_2^{n^*} e^*_{ii-1}$ and $T = Z[a, u^*]$. Then, A^* is T-A^*-irreducible (Lemma 8.4), and so T is a simple ring (Prop.

3.8 (a)). Hence, in virtue of Prop. 8.2 (a), it follows $T \supset Z[E^*, \{x_{ij}\}] = Z[E^*, \{x_{ij}\}, c_o] = A^*$, that is, $T = A^*$. Now, $a' = 1 - u^*$ is evidently the desired element.

(b) If $T = Z[a, ye^*_{21}]$ then A^* is T-A^*-irreducible, and so T is simple (Lemma 8.4 and Prop. 3.8 (a)). Hence, Prop. 8.2 (b) yields $T \supset Z[E^*, d, d', y] = Z[E^*, d, d', y, c_o] = A^*$.

(c) If $T = Z[a, xe^*_{21} + ye^*_{22}]$ then $T \cap D^*e^*_{21} \neq 0$ (Lemma 8.6). Hence, A^* is T-A^*-irreducible (Lemma 8.4), and the rest of the proof proceeds just like that of (b) did.

Proposition 8.8. *Let* A *be a unital* (*simple*) *subring of a ring* $S \ni 1$, *and* T *a subring of* S *such that* $T\tilde{A} \subset T$. *If* $Te_{pq} \subset T$ *for some* e_{pq} *then* $TA = T$. (Needless to say, in case T contains 1, $A \subset T$ replaces $TA = T$.)

Proof. If $p \neq q$ then $T \supset (1 = e_{qp})Te_{pq}(1 + e_{qp})^{-1} = T(e_{pq} + e_{qq} - e_{pp} - e_{qp})$ and $T \supset Te_{pq}$ imply $T \supset Te_{pq}(e_{pq} + e_{qq} - e_{pp} - e_{qp}) = T(e_{pq} - e_{pp})$, or, $T \supset Te_{pp}$. Now, for any $i \neq p$ and $d \in D$, we obtain $T \supset (1 + de_{ip})Te_{pp}(1 + de_{ip})^{-1} = T(e_{pp} + de_{ip})$. Accordingly, it follows $T \supset Tde_{ip}$, and similarly $T \supset Tde_{pi}$. Now, it is easy to see $T = TA$.

Corollary 8.9. *Assume that all the assumption in Prop.* 8.8 *are satisfied and that* A *is of characteristic* 2.

(a) *If* $T(x + e_{21}) \subset T$ *for some* $x \in D$ *then* $TA = T$.

(b) *If* $n > 2$ *and* $T(\sum_2^n e_{ii-1} + e_{1n} + e_{1n-1}) \subset T$ *then* $TA = T$.

Proof. Set $a_1 = x + e_{21}$, $a_2 = \sum_2^n e_{ii-1} + e_{1n} + e_{1n-1}$ and $a^* = e_{11} + e_{22} + e_{12}$. In either case, we obtain $T \supset (1 + e_{12})Ta_i(1 + e_{12})^{-1} = T(a_i - a^*)$, whence it follows $T \supset Ta^*$. Hence, $T(a^* - a^{*2}) = Te_{12}$, and then $TA = T$ by Prop. 8.8.

Proposition 8.10. *Let* S *be a ring with* 1, *and* T *a two-sided simple subring of* S.

(a) *Let* A' *be a unital simple subring of* S *different from* $(GF(2))_2$. *If* $T\tilde{A}' \subset T$ *then either* $TA' = T$ *or* $A' \subset V_S(T)$.

(b) Let A' be a unital subring of S, and $2T \neq 0$. If $T\delta_a \subset T$ for every a in A' then either $TA' = T$ or $A' \subset V_S(T)$.

Proof. (a) Let $A' = \sum_1^{n'} D'e'_{ij}$, where $E' = \{e'_{ij}\}$ is a system of matrix units and $D' = V_{A'}(E')$ a division ring. If a is a unit of A' and $\{a, 1\}$ is not left T-free, then $t_1 a - t_2 = 0$ with some $t_1 \neq 0$, $t_2 \in T$, and then, noting that T is two-sided simple and $T\tilde{A}' = T$, one will easily see $Ta \subset T$. Next, if a is biregular (i.e. if a and $1 - a$ are units of A') and $\{a, 1\}$ is left T-free then, for every t in T, $(1 - a)t = t''(1 - a)$ and $at = t'a$ $(t', t'' \in T)$ yield $t = t'' = t'$, whence it follows that a is contained in $V_S(T)$. Particularly, in case A' is a division ring, the above remark shows that for every element a of A' there holds either $Ta \subset T$ or $a \in V_S(T)$. Now, we shall prove our assertion.

Case I. $n' = 1$: If $A' \not\subset V_S(T)$ then there exists an element $a \in A' \setminus V_S(T)$ and $Ta \subset T$ by the last remark. Suppose now that there exists an element $a_o \in A'$ such that $Ta_o \not\subset T$. Then, again by the above remark, a_o and $a + a_o$ are contained in $V_S(T)$, which implies a contradiction $a \in V_S(T)$. Hence, we have $TA' = T$.

Case II. $n' > 1$: One may remark that $V_S(T)\tilde{A}' \subset V_S(T)$. Firstly, if A' is not of characteristic 2 then $a_o = 2 + e'_{21}$ is biregular, and so $Ta_o \subset T$ or $a_o \in V_S(T)$ by the remark mentioned at the beginning. Hence, $Te'_{21} \subset T$ or $e'_{21} \in V_S(T)$, whence it follows $TA' = T$ or $A' \subset V_S(T)$ by Prop. 8.8. Next, if A' is of characteristic 2 and D' is different from $GF(2)$, then $a_1 = x + e'_{21}$ is biregular for any x in D' different from 0 or 1, and hence $Ta_1 \subset T$ or $a_1 \in V_S(T)$ by the same remark. Then, Cor. 8.9 (a) yields at once our assertion. Finally, assume that A' is of characteristic 2 and $n' > 2$. As $a_2 = \sum_2^{n'} e'_{ii-1} + e'_{1n'} + e'_{1n'-1}$ is biregular, our assertion is, this time, a consequence of Cor. 8.9 (b).

(b) Let a be an arbitrary element of A'. Then, for any $t \in T$

we have $[t, a] = ta - at = t_1$, $[[t, a], a] = t_2$ and $[t, a^2] = t_3$ with t_i in T. A brief computation implies then $2t_1a = 2(ta^2 - ata) = t_2 + t_3 \in T$. Accordingly, if $\{a, 1\}$ is left T-free then $t_1 = 0$, or, $a \in V_S(T)$. On the other hand, if $\{a, 1\}$ is not left T-free then it will be easy to see that $Ta \subset T$ by our assumption. We have seen therefore that for every element $a \in A'$ there holds either $a \in V_S(T)$ or $Ta \subset T$. Consequently, the rest of the proof proceeds in the same way as in Case I of (a).

Brauer [1]; Cartan [3]; Hua [1]; Kasch-Tominaga [1]; Kishimoto [1]; Kishimoto-Nagahara-Tominaga [1]; Nagahara-Tominaga [3], [7].

9. Normal basis theorems

If A is a finite Galois extension field over B then it is well known that A possesses a normal basis $\{a\sigma\ ;\ \sigma \in \mathfrak{G}\}$, or equivalently, A is $\mathfrak{G}B_R$-homomorphic to $\mathfrak{G}B_R$. The following theorem asserts that the last proposition is still valid for simple rings.

Theorem 9.1. *Let $\mathfrak{H}$ be an N-group of A with $B = J(\mathfrak{H})$. If N is an $\mathfrak{H}$-invariant right Artinian unital subring of A and A_N is generated by $\{x_1, \cdots, x_t\}$ with $t \leqslant [A;B] < \infty$ (cf. Prop. 7.1) then A is $\mathfrak{H}N_R$-homomorphic to $\mathfrak{H}N_R$. In particular, A is always $\mathfrak{H}B_R$-homomorphic to $\mathfrak{H}B_R$. If moreover $\mathfrak{H}$ is abelian then A is $\mathfrak{H}B_R$-isomorphic to $\mathfrak{H}B_R$.*

Proof. Since $\mathfrak{H}A_R = \oplus_1^m \sigma_i A_R = \sum_{i,j} \sigma_i x_{jR} N_R$ with some $\sigma_i \in \mathfrak{H}$, the subring $\mathfrak{H}N_R$ of $\mathfrak{H}A_R$ satisfies the minimum condition for right ideals. Noting that $\mathfrak{H}A_R = A_R\mathfrak{H} = \sum_1^t x_{jR}N_R\mathfrak{H} = \sum_1^t x_{jR}(\mathfrak{H}N_R)$, $\mathfrak{H}A_R$ is $\mathfrak{H}N_R$-homomorphic to $(\mathfrak{H}N_R)^{(t)}$. On the other hand, as $V_{\mathfrak{G}}(B_L) = \mathfrak{H}A_R$ (Prop. 7.1) and $[A:B] = m$, $A^{(m)}$ is $\mathfrak{H}A_R$-isomorphic to $\mathfrak{H}A_R$ (Th. 2.15). Hence, $A^{(m)}$ is $\mathfrak{H}N_R$-homomorphic to $(\mathfrak{H}N_R)^{(t)}$. It follows therefore A is $\mathfrak{H}N_R$-homomorphic to $\mathfrak{H}N_R$ (Cor. 3.16 (a)). Finally, assume $\mathfrak{H}$ is abelian. Let $\sigma = \sum \sigma_i y_{iR}$ $(y_i \in A)$ be an arbitrary element of $\mathfrak{H}$. Then for every $\tau \in \mathfrak{H}$ there holds $\sum \tau\sigma_i y_{iR} = \tau\sigma = \sigma\tau = \sum \tau\sigma_i (y_i\tau)_R$, whence it follows $y_i = y_i\tau$. We see thus every y_i is contained in B, namely, $\mathfrak{H}B_R = \oplus_1^m \sigma_i B_R$. Now, the final isomorphism is evident.

Lemma 9.2. *Let $\mathfrak{H}$ be an N-group of A with $B = J(\mathfrak{H})$, $[A:B] = m$, and N an $\mathfrak{H}$-invariant right Artinian unital subring of A such that A possesses a right N-basis $\{x_\lambda\ ;\ \lambda \in \Lambda\}$. If $V = C$ or $V \subset N$ then $\mathfrak{H}N_R$ possesses a right N_R-basis consisting of m elements of $\mathfrak{H}$ and $\{x_{\lambda R};\ \lambda \in \Lambda\}$ forms a right $\mathfrak{H}N_R$-basis of $\mathfrak{H}A_R$.*

Proof. As in the proof of Th. 9.1, $A^{(m)}$ is $\mathfrak{H}A_R$-isomorphic to

$\mathfrak{G}A_R$ and $V_{\mathfrak{a}}(B_L) = \mathfrak{G}A_R = \oplus_1^m \sigma_i A_R = \oplus_1^m A_R\sigma_i$ with some $\sigma_i \in \mathfrak{G}$ If $V = C$ then $\{\sigma_1, \cdots, \sigma_m\}$ coincides with $\mathfrak{G}$ (Th. 7.4). On the other hand, if $V \subset N$ then $\mathfrak{G}V_R = \oplus_1^m \sigma_i V_R \subset \oplus_1^m \sigma_i N_R$ (Prop. 5.7 (b)). Thus, in either case, $\mathfrak{G}N_R = \oplus_1^m \sigma_i N_R$ and $\mathfrak{G}A_R = \oplus_{i,\lambda} x_{\lambda R} N_R \sigma_i = \oplus_\lambda x_{\lambda R}(\mathfrak{G}N_R)$, namely, $\{x_{\lambda R}; \lambda \in \Lambda\}$ is a right $\mathfrak{G}N_R$-basis of $\mathfrak{G}A_R$.

Lemma 9.3. Let A be finite Galois over B, $V \neq (GF(2))_2$, and N a $\mathfrak{G}$-invariant unital simple subring of A. If $[\mathfrak{G}N_R:N_R]_R = [A:B]$ then $V = C$ or $V \subset N$.

Proof. Suppose on the contrary that V is neither C nor contained in N. Every element of V is a finite sum of elements in V^* (Prop. 3.5) and $[\mathfrak{G}A_R:A_R]_R = [A:B]$ (Prop. 7.1). In what follows, we shall prove that there exist some $v, v_1, \cdots, v_k$ in V^* such that $\{v_1, \cdots, v_k\}$ is C-free and $\tilde{v} = \sum_1^k \tilde{v}_i a_{iR}$ with some $a_i \in A$ not all contained in N, which implies $[\mathfrak{G}A_R:A_R]_R < [\mathfrak{G}N_R:N_R]_R$. To this end, we set $V = \sum_1^r Ug_{pq}$ and distinguish between two cases.

Case I. $r = 1$: Let $\{v_1 = 1, v_2, \cdots, v_m\}$ be a C-basis of V. Then, $V \neq C$ implies $m > 1$. We distinguish further between two cases:

(i) $C \not\subset N$: Let c be an arbitrary element of $C \backslash N$. If $v = 1 + v_2$ and $v' = 1 + cv_2$ then $\tilde{v} = \tilde{1}v_R^{-1} + \tilde{v}_2(v_2 v^{-1})_R$ and $\tilde{v}' = \tilde{1}v'^{-1}_R + \tilde{v}_2(v_2 c v'^{-1})_R$. Suppose that both v and v' are in N. Then, $(v - 1)v_1 = v_2 = c^{-1}(v' - 1)v_1$ yields a contradiction $c = (v - 1)(v' - 1)^{-1} \in N$. Hence, one of v^{-1}, v'^{-1} does not belong to N.

(ii) $C \subset N$: As $C \subset N$ and $V \not\subset N$, without loss of generality, we may assume that $v_2 \notin N$. Then, for $v = 1 + v_2$ we have $\tilde{v} = \tilde{1}v_R^{-1} + \tilde{v}_2(v_2 v^{-1})_R$ and $v^{-1} \notin N$.

Case II. $r > 1$: The set $\{1, f_{pq} = 1 - g_{pq}\ (p, q = 1, 2, \cdots, r;\ p \neq q\}$ contained in V^* is C-free, and in case r is even so is the set $\{f_q = g_{qq} + \sum_{p=1}^r g_{p\ r-p+1}\ (q = 1, 2, \cdots, r)\}$. Since $N\tilde{V} \subset N$ and $V \not\subset N$, N is contained in H by Prop. 8.10. Noting

that $V \cap N$ is then contained in the center of V, it is obvious that no non-diagonal elements of V are contained in N. Now, we shall distinguish between two cases:

(i) V is not of characteristic 2: In this case, every $f'_{pq} = 1 + f_{pq}$ is in V^* and $\tilde{f}'_{pq} = \tilde{1}(f'^{-1}_{pq})_R + \tilde{f}_{pq}(f_{pq}f'^{-1}_{pq})_R$ with $f'^{-1}_{pq} \notin N$.

(ii) V is of characteristic 2: If r is odd then $u = 1 + \sum_2^r f_{p-1p}$ is in V^* and $\tilde{u} = \tilde{1}u_R^{-1} + \sum_2^r \tilde{f}_{p-1p}(f_{p-1p}u^{-1})_R$ with $u^{-1} \notin N$. On the other hand, if r is even then $1 = \sum_1^r f_p$ and $\tilde{1} = \sum_1^r \tilde{f}_p f_{pR}$ with $f_p \notin N$.

In the proof of Lemma 9.3, the assumption $V \neq (GF(2))_2$ was needed only to secure that N is contained in H provided V is not contained in N. Accordingly, for $N = B$ Lemma 9.3 is valid without the assumption $V \neq (GF(2))_2$. However, the assumption is indispensable in Lemma 9.3 (cf. Kishimoto-Onodera-Tominaga [1]).

Theorem 9.4. *Let A be finite Galois over B, $V \neq (GF(2))_2$, and N a $\mathcal{G}$-invariant unital simple subring of A.*

(a) The following conditions are equivalent: (1) $V = C$ *or* $V \subset N$, *and* (2) $[\mathcal{G}N_R : N_R]_R = [A:B]$.

(b) If $[A:N]_R$ is an infinite cardinal number ω and any of the conditions (1), (2) *cited in* (a) *is satisfied then A is $\mathcal{G}N_R$-isomorphic to $(\mathcal{G}N_R)^{(\omega)}$.*

(c) If $[A:N]_R = t$ and $t = mq + r$ $(0 \leq r < m = [A:B])$ then each of the conditions (1), (2) *cited in* (a) *is equivalent to the following:* (3) *A is $\mathcal{G}N_R$-isomorphic to $(\mathcal{G}N_R)^{(q)} \oplus \mathfrak{m}$, where $\mathfrak{m}$ is a $\mathcal{G}N_R$-homomorphic image of $\mathcal{G}N_R$ such that $\mathfrak{m}^{(m)}$ is $\mathcal{G}N_R$-isomorphic to $(\mathcal{G}N_R)^{(r)}$.*

Proof. (a) is a direct consequence of Lemmas 9.2 and 9.3. Further, as $A^{(m)}$ is $\mathcal{G}A_R$-isomorphic to $\mathcal{G}A_R$ (cf. the proof of Th. 9.1), the latter half of Lemma 9.2 together with Cor. 3.16 (b) or Cor. 3.16 (c) yields at once (b) or (c).

Corollary 9.5. Let A be finite Galois over B.

(a) The following conditions are equivalent: (1) $V = C$ or $V \subset B$, (2) $[\mathfrak{G} B_R : B_R]_R = [A:B]$, and (3) A is $\mathfrak{G} B_R$-isomorphic to $\mathfrak{G} B_R$.

(b) If $\mathfrak{G}$ is abelian and $[B:Z] < \infty$ then A/B is either outer Galois or inner Galois. In particular, if $\mathfrak{G}$ is abelian and B is a field then A is a field or B coincides with V.

Proof. By the remark stated just after Lemma 9.3, we readily obtain (a). If $\mathfrak{G}$ is abelian then $V = C$ or $V \subset B$ by Th. 9.1 and (a). Since $[B:Z] < \infty$ yields $[A:C] < \infty$ (Cor. 7.11), (b) is a consequence of Th. 7.7 and Cor. 4.9.

If $\mathfrak{H}$ is an F-group of A and $B = J(\mathfrak{H})$, we have seen in § 7 that A/B is Galois and $[A:B] \leq \#\mathfrak{H}$. We shall introduce here the following definition: If $\mathfrak{H}$ is an F-group of A with $B = J(\mathfrak{H})$ and $[A:B]$ coincides with $\#\mathfrak{H}$, then A is said to be $\mathfrak{H}$-regular or A/B is $\mathfrak{H}$-regular. It is clear that if A is outer Galois and finite over B then A/B is $\mathfrak{H}$-regular.

Proposition 9.6. Let $\mathfrak{H}$ be an F-group of A and $B = J(\mathfrak{H})$. Then, the following conditions are equivalent: (1) A/B is $\mathfrak{H}$-regular, (2) $\mathfrak{H}$ is free over A_R and (3) there exist some $x_1, \cdots, x_t; y_1, \cdots, y_t$ in A such that $\sum_i y_i\sigma \cdot x_i = \delta_{1\sigma}$ ($\sigma \in \mathfrak{H}$). If A/B is $\mathfrak{H}$-regular then $\mathrm{Hom}({}_BA, {}_BB) = A_R \cdot \sum_{\sigma \in \mathfrak{H}} \sigma$.

Proof. (1) $\Longleftrightarrow$ (2) is obvious by Prop. 7.1. (2) $\Longrightarrow$ (3): If $f = \sum_\sigma \sigma a_{\sigma R}$ is in $\mathrm{Hom}({}_BA, {}_BB)$ then for every $\tau \in \mathfrak{H}$ we have $\sum_\sigma \sigma\tau(a_{\sigma\tau})_R = f\tau = f = \sum_\sigma \sigma a_{\sigma R}$, whence it follows $a_1\tau = a_\tau$. Hence, it follows $f = a_{1R} \cdot \sum_\sigma \sigma$. Now, let $\{f_1, \cdots, f_t\}$ be an A_R-basis of $V_{\mathfrak{A}}(B_L)$ contained in $\mathrm{Hom}({}_BA, {}_BB)$ (Prop. 2.6). Since $f_i = y_{iR} \cdot \sum_\sigma \sigma$ and $\sum_1^t f_i x_{iR} = 1$ for some x_i and y_i in A, one will easily see that $\sum_i y_i\sigma \cdot x_i = \delta_{1\sigma}$. (3) $\Longrightarrow$ (2): If $\sum_\sigma \sigma a_{\sigma R} = 0$ ($a_\sigma \in A$) then for every $\tau \in \mathfrak{H}$ we have $0 = \sum_i y_{iR}\tau(\sum_\sigma x_i\sigma \cdot a_\sigma)_R = \sum_\sigma (\sum_i y_{iR}\tau\sigma^{-1}x_{iR})\sigma a_{\sigma R} = \tau a_{\tau R}$, namely, $a_\tau = 0$.

Next, we shall give another approach to the classical normal basis theorem.

Theorem 9.7. Let A/B be $\mathfrak{G}$-regular, $\#\mathfrak{G} = h$, and let N be an $\mathfrak{G}$-invariant right Artinian unital subring of A such that A possesses a right N-basis $\{u_\lambda ; \lambda \in \Lambda\}$.

(a) If Λ is infinite then there exists a subset $\{x_\lambda ; \lambda \in \Lambda\}$ of A such that $\{x_\lambda\sigma ; \lambda \in \Lambda , \sigma \in \mathfrak{G}\}$ is a right N-basis of A.

(b) If $\#\Lambda = t = hq + r$ $(0 \leq r < h)$ then A contains q elements $x_1, \cdots, x_q$ and an $\mathfrak{G}N_R$-homomorphic image M of $\mathfrak{G}N_R$ such that $\{x_i\sigma ; i = 1, \cdots, q, \sigma \in \mathfrak{G}\}$ is right N-free, $M^{(h)}$ is $\mathfrak{G}N_R$-isomorphic to $(\mathfrak{G}N_R)^{(r)}$ and $A = (\oplus_{i,\sigma} (x_i\sigma)N) \oplus M$.

Proof. Since $V_{\sigma\tau}(B_L) = \mathfrak{G}A_R = \oplus_{\sigma \in \mathfrak{G}} \sigma A_R$, there holds $\mathfrak{G}N_R = \oplus_\sigma \sigma N_R$. Hence, as in the proof of Lemma 9.2, we see that $\mathfrak{G}N_R$ is a right Artinian subring of $\mathfrak{G}A_R$ and $A^{(h)}$ is $\mathfrak{G}N_R$-isomorphic to $(\mathfrak{G}N_R)^{(\#\Lambda)}$. Our assertions are then consequences of Cor. 3.16 (b) and (c).

Applying Th. 9.7 to the case that A is a division ring, we obtain the following at once:

Corollary 9.8. Let a division ring A be $\mathfrak{G}$-regular with of order h, and let N be an $\mathfrak{G}$-invariant division subring of A. If $[A:N]_R = t = hq + r$ $(0 \leq r < h)$ then there exist $q + 1$ elements $x_0, x_1, \cdots, x_q$ in A such that $A = (\oplus_{i=1}^{q}(\oplus_{\sigma \in \mathfrak{G}} x_i\sigma \cdot N)) \oplus (\oplus_j x_0\sigma_j \cdot N)$, where σ_j ranges over suitable r elements of $\mathfrak{G}$.

The next is the special case of Th. 9.7 for $N = B$.

Corollary 9.9. If A/B is $\mathfrak{G}$-regular then there exists an element a in A such that $\{a\sigma ; \sigma \in \mathfrak{G}\}$ is a right (resp. left) B-basis of A. Such a B-basis $\{a\sigma ; \sigma \in \mathfrak{G}\}$ and such an element a will be called a right (resp. left) $\mathfrak{G}$-normal basis of A/B and a right (resp. left) $\mathfrak{G}$-normal basis element (abbreviated $\mathfrak{G}$-n.b.e.), respectively. If a is a right $\mathfrak{G}$-n.b.e., then $T_{\mathfrak{G}}(a) = \sum_{\sigma \in \mathfrak{G}} a\sigma$ is in B^*, and so $T_{\mathfrak{G}}(A) = \{T_{\mathfrak{G}}(x); x \in A\} = B$.

The next is well known for the commutative case.

Theorem 9.10. Let $\mathfrak{G} = \{\sigma_1, \ldots, \sigma_h\}$ be an F-group of A with $B = J(\mathfrak{G})$. In order that an element a in A be a left $\mathfrak{G}$-n.b.e. (resp. a right $\mathfrak{G}$-n.b.e.), it is necessary and sufficient that the matrix $(a\sigma_i\sigma_j)$ (resp. the matrix transposed ${}^t(a\sigma_i\sigma_j)$) be regular.

Proof. The sufficiency is easy. We shall prove the necessity, and assume that a be a left $\mathfrak{G}$-n.b.e. By Prop. 9.6, we can find $f_k = y_{kR} \cdot \sum_j \sigma_j$ in $A_R \cdot \sum_j \sigma_j$ such that $\sum_j a\sigma_i\sigma_j \cdot y_k\sigma_j = a\sigma_i f_k = \delta_{ik}$ $(i, k = 1, \ldots, n)$. Hence, $(a\sigma_i\sigma_j)$ is regular.

Faith [4]; Kasch [6]; Kishimoto-Onodera-Tominaga [1], Nagahara-Onodera-Tominaga [1]; Onodera [1]; Tominaga [6].

10. Witt's theorem and Noether-Speiser's theorem

Let R be a ring with 1, and $\mathfrak{G}$ a finite group of ring automorphisms of R such that $T_{\mathfrak{G}}(a) = 1$ for some $a \in R$. If for every $\sigma \in \mathfrak{G}$ there corresponds an element x_σ in R and there holds $x_\tau + x_{\sigma\tau} = x_{\sigma\tau}$ $(\sigma, \tau \in \mathfrak{G})$, then there exists an element x in R such that $x_\sigma = -x + x\sigma$. In fact, a direct computation will show that $x = -\sum_{\tau \in \mathfrak{G}} x_\tau \cdot a_\tau$ satisfies the relation proposed. In particular, by the validity of Cor. 9.9, we obtain the following generalization of Witt's theorem.

Theorem 10.1. *Let A/B be $\mathfrak{G}$-regular. If for every $\sigma \in \mathfrak{G}$ there corresponds an element x_σ in A and there holds $x_\tau + x_{\sigma\tau} = x_{\sigma\tau}$ $(\sigma, \tau \in \mathfrak{G})$, then there exists an element x in A such that $x_\sigma = -x + x\sigma$, and conversely. In particular, if $\sigma \longrightarrow x_\sigma$ is a homomorphism of $\mathfrak{G}$ into the additive group of B then there exists an element x in A such that $x_\sigma = -x + x\sigma$.*

Lemma 10.2. *Let A/B be $\mathfrak{G}$-regular, and $\mathfrak{N}$ an F-subgroup of $\mathfrak{G}$. If $N = J(\mathfrak{N})$ then A/N is $\mathfrak{N}$-regular, $[N:B] = (\mathfrak{G} : \mathfrak{N})$ and $\mathfrak{G}(N) = \mathfrak{N}$. In particular, if $\mathfrak{N}$ is an invariant F-subgroup of $\mathfrak{G}$ then $N|\mathfrak{G} \simeq \mathfrak{G}/\mathfrak{N}$.*

Proof. Since A/N is $\mathfrak{N}$-regular by Prop. 9.6, we obtain $\#\mathfrak{G} = \#\mathfrak{N} \cdot (\mathfrak{G} : \mathfrak{N}) \geqq [A:N] \cdot [(N|\mathfrak{G})A_R : A_R]_R = [A:N] \cdot [N:B] = [A:B] = \#\mathfrak{G}$. Our assertions are consequences of the last relation.

Lemma 10.3. *Let A be a central simple algebra of finite rank over C, $\mathfrak{G}$ an automorphism group of A such that $J(\mathfrak{G}) = C$ and $\#\mathfrak{G} = p^e$ (p a prime). If C contains no primitive p-th roots of 1 then $A = C$.*

Proof. Suppose on the contrary $e > 0$. As $\mathfrak{G}(A/C) = \tilde{A}$ (Th. 7.7), the center of $\mathfrak{G}$ contains a subgroup $\mathfrak{P} = \{\tilde{1}, \tilde{v}, \ldots, \tilde{v}^{p-1}\}$ of order p. Then, for every $\sigma = \tilde{u} \in \mathfrak{G}$, $\tilde{v}\sigma = \sigma\tilde{v}$ implies $v\sigma = vc_\sigma$ with some $c_\sigma \in C$. Accordingly, $v^p = uv^p u^{-1} = (v\sigma)^p = v^p c_\sigma^p$, whence it follows $c_\sigma^p = 1$, i.e., $c_\sigma = 1$, which means obviously $v\sigma = v$. Hence, v is contained in $J(\mathfrak{G}) = C$, namely, $\tilde{v} = 1$.

Lemma 10.4. Let $\mathfrak{G}$ be an F-group of A with $\#\mathfrak{G} = p^e$ (p a prime) and $B = J(\mathfrak{G})$. If Z contains no primitive p-th roots of 1 then V coincides with the field $C \cdot Z$.

Proof. Let $\mathfrak{G}_0 = \mathfrak{G} \cap \tilde{A}$. Then, $V = I(\mathfrak{G}) = I(\mathfrak{G}_0)$ and $[V:C] < \infty$ (Prop. 7.1). Obviously, $C_0 | \mathfrak{G}$ is the Galois group of C_0/Z, and so $[C_0:Z] = \#(C_0|\mathfrak{G})$ divides p^e. Hence, C_0 contains no primitive p-th roots of 1. Since $V | \mathfrak{G}_0$ is an automorphism group of V such that $\#(V | \mathfrak{G}_0)$ divides p^e and $J(V | \mathfrak{G}_0) = C_0$, Lemma 10.3 yields then $V = C_0$. Suppose now $V \supsetneqq C \cdot Z$, and choose an element $v \in V \setminus C \cdot Z$ such that $\tilde{v} \in \mathfrak{G}_0$. Noting that the field V is Galois and finite over $C \cdot Z$ and the p^e-th power of v is contained in C, we can find an element $u \neq v$ in V such that $u^{p^e} = v^{p^e}$. However, as $C_0 = V$ contains no primitive p-th roots of 1, this is impossible.

Theorem 10.5. Let A be of characteristic $p \neq 0$, and $\mathfrak{G} = \mathfrak{G}_1 \times \cdots \times \mathfrak{G}_e$ an F-group of A, where every $\mathfrak{G}_i$ is a cyclic subgroup generated by σ_i of order p. If A/B is $\mathfrak{G}$-regular then there exist some $x_1, \cdots, x_e$ in A such that (1) $x_i^{\mathfrak{G}} = x_i^p - x_i \in B$, (2) the inner derivation δ_{x_i} induces a derivation ∂_i in B such that $\partial_i^{\mathfrak{G}}$ is inner, (3) $A = B[x_1, \cdots, x_e]$, (4) $B = B[x_i] \cap B[x_1, \cdots, \overset{\vee}{x_i}, \cdots, x_e]$ and (5) $B[x_i]/B$ is $\mathfrak{G}_i$-regular.

Proof. As $V = I(\mathfrak{G})$ is a field (Lemma 10.4), every intermediate ring of A/B is simple by Prop. 7.3. For every i, $\sigma = \prod_j \sigma_j^{t_j} \longrightarrow t_i$ defines a homomorphism of $\mathfrak{G}$ into the additive group of B. Hence, there exists an element x_i in A such that $x_i\sigma_i = x_i + 1$ and $x_i\sigma_j = x_i$ for every $j \neq i$ (Th. 10.1). It is obvious that $\partial_i = B | \delta_{x_i}$ is a derivation of B. Since $(x_i^p)\sigma_i = x_i^p + 1$, we obtain $x_i^{\mathfrak{G}}\sigma_i = x_i^{\mathfrak{G}}$, whence it follows $x_i^{\mathfrak{G}} \in B$ and $\partial_i^{\mathfrak{G}}$ is inner. Now, in virtue of Lemma 10.2, we can see that $B[x_1, \cdots, x_i] = J(\mathfrak{G}_{i+1} \times \cdots \times \mathfrak{G}_e)$, and hence the rest of the proof is evident.

Corresponding to Th. 10, we shall give an extension of Noether-Speiser's theorem.

Theorem 10.6. Let A/B be $\mathfrak{G}$-regular. If for every $\sigma \in \mathfrak{G}$ there corresponds an element $x_\sigma \in A^\cdot$ and there holds $x_\tau \cdot x_\sigma{}^\tau = x_{\sigma\tau}$ $(\sigma, \tau \in \mathfrak{G})$, then there exists an element $x \in A^\cdot$ such that $x_\sigma = x^{-1} \cdot x\sigma$, and conversely. In particular, if $\sigma \longrightarrow x_\sigma$ is an anti-homomorphism of $\mathfrak{G}$ into $B^\cdot$ then there exists an element $x \in A^\cdot$ such that $x\sigma = xx_\sigma$.

Proof. Evidently, $\theta_\sigma = \sigma x_{\sigma L}$ is a 1-1 A_R-semilinear transformation of A belonging to the automorphism σ. The assumption $x_\tau \cdot x_{\sigma\tau} = x_{\sigma\tau}$ yields then $\theta_\sigma \theta_\tau = \theta_{\sigma\tau}$, whence we have especially $\theta_1 = 1$. Hence, $\mathfrak{A}' = \sum_\sigma \theta_\sigma A_R$ is an intermediate ring of $\mathfrak{A}/A_R$. Since $V_{\mathfrak{A}}(B_L) = \mathfrak{G} A_R = \bigoplus_{\sigma \in \mathfrak{G}} \sigma A_R$ is simple (Prop. 7.1) and $\phi : \sum \sigma u_{\sigma R} \longrightarrow \sum \theta_\sigma u_{\sigma R}$ is an A_R-ring homomorphism of $\mathfrak{G} A_R$ onto $\mathfrak{A}'$, ϕ has to be an isomorphism. Accordingly, ϕ can be extended to an inner automorphism $\tilde{\eta}$ of $\mathfrak{A}$ by Th. 3.11. As ϕ is an A_R-isomorphism, $\eta = x_L$ for some $x \in A^\cdot$ and $\sigma x_L^{-1} = x_L^{-1}\theta_\sigma = x_L^{-1}\sigma x_{\sigma L} = \sigma(x^{-1}\sigma)_L x_{\sigma L}$. We obtain therefore our assertion $x_\sigma = x^{-1} \cdot x\sigma$.

If A/B is $\mathfrak{G}$-regular, then $\mathfrak{G}$ may be regarded naturally as an F-group of $(A)_m$, and then $(A)_m/(B)_m$ is $\mathfrak{G}$-regular. Accordingly, we obtain the following generalization of von Neumann's theorem.

Corollary 10.7. Let A/B be $\mathfrak{G}$-regular. If for every $\sigma \in \mathfrak{G}$ there corresponds a regular matrix $X_\sigma \in (A)_m$ and there holds $X_\tau \cdot (X_\sigma{}^\tau) = X_{\sigma\tau}$ $(\sigma, \tau \in \mathfrak{G})$, then there exists a regular matrix X in $(A)_m$ such that $X_\sigma = X^{-1} \cdot (X\sigma)$, and conversely.

The next is well known, and an easy consequence of Th. 10.6.

Corollary 10.8. If $B = GF(q)$ and $A = GF(q^m)$ then $N_{A/B}(A) = B$.

Now, as an application of Th. 10.6, we shall develop a Kummer-like theory for simple rings. To this end, we shall prove first the following:

Lemma 10.9. Let $\mathfrak{G} = [\sigma]$ be a cyclic F-group of A with the generator σ of order m, $B = J(\mathfrak{G})$, and the field $B \cap C$ contain a

a primitive m-th root ζ of 1. If there exists an element a in A^* such that $a\sigma = a\zeta$ then $A = \bigoplus_0^{m-1} Ba^i = \bigoplus_0^{m-1} a^iB$.

Proof. Assume that $f(x) = b_0x^t + b_1x^{t-1} + \ldots + b_t$ $(b_0 \neq 0)$ is a polynomial with coefficients in B such that $f(a) = 0$. Noting that $0 = f(a)\sigma^i = b_0a^t(\zeta^i)^t + b_1a^{t-1}(\zeta^i)^{t-1} + \ldots + b_t$ for $i = 0, 1, \ldots, m-1$, $t < m$ implies a contradiction $b_0 = 0$. Hence, $t \geqslant m$, whence it follows $\sum_0^{m-1} Ba^i = \bigoplus_0^{m-1} Ba^i$. Since $[A:B] \leqslant m$ (§ 7), we obtain eventually $A = \bigoplus_0^{m-1} Ba^i$, and similarly $A = \bigoplus_0^{m-1} a^iB$.

Let $\mathfrak{G}$ be a commutative DF-group of A whose exponent is m_0. If A/B is $\mathfrak{G}$-regular and $B \cap C$ contains a primitive m_0-th root of 1 then A/B is called an $\mathfrak{G}$-Kummer extension. The next theorem will guarantee that the notion is a generalization of the classical one for fields.

Theorem 10.10. Let A/B be an $\mathfrak{G}$-Kummer extension. If $\mathfrak{G} = \mathfrak{G}_1 \times \cdots \times \mathfrak{G}_e$ with cyclic $\mathfrak{G}_i = [\sigma_i]$ of order m_i, then there exist some $x_1, \ldots, x_e$ in A^* such that (1) $x_i^{m_i} \in B$, (a) $\tilde{x}_i^{-1}$ induces an automorphism τ_i in B such that $\tau_i^{m_i}$ is inner (3) $A = B[x_1, \ldots, x_e]$, (4) $B[x_i] \cap B[x_1, \ldots, \check{x}_i, \ldots, x_e] = B$, (5) $B[x_i]/B$ is an $\mathfrak{G}_i$-Kummer extension and (6) if G is the subgroup of A^* generated by $x_1, \ldots, x_e$ then $G \cap B$ is an invariant subgroup of G and $G/(G \cap B)$ is isomorphic to .

Proof. Let ζ be a primitive m_0-th root of 1 contained in $B \cap C$, and let $\zeta_i = \zeta^{m_0/m_i}$, that is evidently a primitive m_i-th root of 1. For every i, the mapping $\sigma = \prod_j \sigma_j^{t_j} \longrightarrow \zeta_i^{t_i}$ defines a homomorphism of $\mathfrak{G}$ into $(B \cap C)^*$, and so there exists an element x_i in A^* such that $x_i\sigma_i = x_i\zeta_i$ and $x_i\sigma_j = x_i$ for every $j \neq i$ (Th. 10.6). Evidently, $x_i^{m_i} = (x_i^{m_i})\sigma$ for every $\sigma \in \mathfrak{G}$ and $(x_i^{-1}bx_i)\sigma = x_i^{-1}bx_i$ for every $b \in B$ and $\sigma \in \mathfrak{G}$, which proves (2) and that $G \cap B$ is an invariant subgroup of G. Next, it is easy to see that

$(x_i^{-1}x_j^{-1}x_ix_j)\sigma = x_i^{-1}x_j^{-1}x_ix_j$ for every $\sigma \in \mathfrak{G}$, or what is the same, that $G/(G \cap B)$ is abelian. Noting that $J(\mathfrak{G}_2 \times \ldots \times \mathfrak{G}_e)$ contains x_1 and $\mathfrak{G}_1$-regular (Lemma 10.2), Lemma 10.9 yields at once $J(\mathfrak{G}_2 \times \ldots \times \mathfrak{G}_e) = \bigoplus_0^{m_1-1} Bx_1^i = B[x_1]$. Repeating similar arguments, we obtain $J(\mathfrak{G}_{j+1} \times \ldots \times \mathfrak{G}_e) = \bigoplus_{i=0}^{m_j-1} J(\mathfrak{G}_j \times \ldots \times \mathfrak{G}_e)x_j^i = B[x_1, \ldots, x_j]$, in particular, $A = B[x_1, \ldots, x_e]$. We have proved thus (1) - (5). Since $B[x_j] = \bigoplus_{i=0}^{m_j-1} Bx_j^i$, the isomorphism in (6) is now a consequence of (1) and (4).

In Th. 10.10, if A is a field then $G \cdot B^*$ coincides with $A^* = \{a \in A^*; a^{m_0} \in B\}$. In fact, if a is an arbitrary element of A^* then $x_\sigma = a^{-1} \cdot a\sigma$ is an m_0-th root of 1, and $\sigma \longrightarrow x_\sigma$ is a homomorphism of $\mathfrak{G}$ into B^* (Th. 10.6). Hence, $x_{\sigma_i} = \zeta_i^{\gamma_i}$ with some γ_i ($i = 1, \ldots, e$), and we see that $a \longrightarrow \prod \sigma_j^{\gamma_j}$ is a homomorphism of A^* into $\mathfrak{G}$ with the kernel B^*. Noting that $G \cdot B^* \subset A^*$ and $G \cdot B^*/B^* \simeq G/(G \cap B) \simeq \mathfrak{G}$ (Th. 10.10), we readily obtain $G \cdot B^* = A^*$.

The following theorem gives a condition for an $\mathfrak{G}$-regular extension to be an $\mathfrak{G}$-Kummer extension.

Theorem 10.11. *Let $\mathfrak{G} = \{\eta_1, \ldots, \eta_h\}$ be a DF-group of A whose exponent is m_0, and let A/B be $\mathfrak{G}$-regular. If A/B is an $\mathfrak{G}$-Kummer extension then $A = \bigoplus_1^h a_i B$ with some $a_i \in A^*$ such that every $\zeta_{ij} = a_i^{-1} \cdot a_i \eta_j$ is contained in $B \cap C$, and conversely.*

Proof. Let $\mathfrak{G} = \mathfrak{G}_1 \times \ldots \times \mathfrak{G}_e$ with cyclic $\mathfrak{G}_i = [\sigma_i]$ of order m_i, ζ a primitive m_0-th root of 1 contained in $B \cap C$. If $\zeta_i = \zeta^{m_0/m_i}$ then, as in the proof of Th. 10.10, there exist some $x_1, \ldots, x_e$ in A^* such that $x_i\sigma_i = x_i\zeta_i$ and $x_i\sigma_j = x_i$ for $j \neq i$ and that $A = \bigoplus_{0 \leq t_i < m_i} x_e^{t_e} \ldots x_1^{t_1} \cdot B$. If $\eta = \prod \sigma_i^{s_i}$ ($0 \leq s_i < m_i$) and $a = x_e^{t_e} \ldots x_1^{t_1}$ then $a\eta = a\zeta_e^{t_e s_e} \ldots \zeta_1^{t_1 s_1}$, and so $a^{-1} \cdot a\eta$ is contained in $B \cap C$. Conversely, assume that $A =$

$\oplus_1^h a_iB$ $(a_i \in A^*)$ and every ζ_{ij} is contained in $B \cap C$. We have then $\zeta_{ij}^k = \zeta_{ij}\cdot\zeta_{ij}\eta_j\cdot \cdots \cdot\zeta_{ij}\eta_j^{k-1} = a_i^{-1}\cdot a_i\eta_j^k$ $(k = 0, 1, \cdots)$. If k_j is the order of η_j then $\zeta_{ij}^{k_j} = 1$, whence it follows that some one among the products of $\zeta_{1j}, \cdots, \zeta_{hj}$ is a primitive k_j-th root of 1. Hence, $B \cap C$ contains a primitive m_o-th root of 1. Next, if $a = \sum a_ib_i$ $(b_i \in B)$ is an element of A then $a\eta_s\eta_t = \sum a_ib_i\zeta_{it}\zeta_{is} = a\eta_t\eta_s$ which,asserts that $\mathfrak{G}$ is abelian.

By the proof of Ths. 10.10 and 10.11, one will easily see the following:

Corollary 10.12. *Let A/B be an $\mathfrak{G}$-Kummer extension. If $\mathfrak{G} = \mathfrak{G}_1 \times \mathfrak{G}_2$ and $B_i = J(\mathfrak{G}_i)$ $(i = 1, 2)$, then $A = B_1\cdot B_2 = B_2\cdot B_1$ and every $\mathfrak{G}_2$-n.b.e. of B_1/B is an $\mathfrak{G}_2$-n.b.e. of A/B_2.*

Corollary 10.13. *Let A/B be an $\mathfrak{G}$-Kummer extension with a basis $\{a_1, \cdots, a_h\}$ described in Th. 10.11. In order that $a = \sum a_ib_i$ $(b_i \in B)$ be an $\mathfrak{G}$-n.b.e., it is necessary and sufficient that every b_i be in B^*.*

Proof. By assumption, $a\eta_j = \sum a_i\eta_j\cdot b_i = \sum a_ib_i\zeta_{ij}$. Hence, a is an $\mathfrak{G}$-n.b.e. if and only if the matrix $(b_i\zeta_{ij}) = \mathrm{diag}\{b_1, \cdots, b_h\}\cdot(\zeta_{ij})$ is regular. In virtue of Cor. 9.9, there exists an $\mathfrak{G}$-n.b.e., and so we see that the matrix (ζ_{ij}) is regular. Thus, a is an $\mathfrak{G}$-n.b.e. if and only if the diagonal matrix $\mathrm{diag}\{b_1, \cdots, b_h\}$ is regular, namely, if and only if every b_i is in B^*.

Lemma 10.14. *Let A be a division ring, A/B an $\mathfrak{G}$-Kummer extension, and $\mathfrak{G} = \mathfrak{G}_1 \times \mathfrak{G}_2$ with cyclic $\mathfrak{G}_1 = [\sigma_1]$ of order m'. If $\mathfrak{G}_o$ is a subgroup of $\mathfrak{G}$ containing $\mathfrak{G}_2$, then every $\mathfrak{G}$-n.b.e. of A/B is an $\mathfrak{G}_o$-n.b.e. of $A/J(\mathfrak{G}_o)$.*

Proof. Let $B_i = J(\mathfrak{G}_i)$ $(i = 0, 1, 2)$ and $\mathfrak{G}_1^* = \mathfrak{G}_o \cap \mathfrak{G}_1 = [\sigma_1^s]$ with a positive divisor s of m. Then $\mathfrak{G}_o = \mathfrak{G}_1^* \times \mathfrak{G}_2$. To

be easily seen from the proof of Th. 10.11, there exist some (non-zero) $a_1 = 1, a_2, \cdots, a_m \in B_1^*$ and $a \in B_2^*$ such that $A = \bigoplus a_i a^j B$ $(1 \leqq i \leqq m, 0 \leqq j < m')$, $a_i^{-1} \cdot a_i \eta \in B \cap C$ for every $\eta \in \mathfrak{G}_2$ and $a\sigma_1 = a\zeta'$ with a primitive m'-th root ζ' of 1 contained in $B \cap C$. If $n' = m'/s$ then $a^{n'}\sigma_1^s = a^{n'}$, and so $\{a^{n'\lambda} ; 0 \leqq \lambda < s\}$ forms a right B-basis of B_0. It follows therefore $\{a_i a^\mu ; 1 \leqq i \leqq m, 0 \leqq \mu < n'\}$ is a right B_0-basis of A and $(a_i a^\mu)^{-1} \cdot (a_i a^\mu)\eta \in B \cap C$ for every $\eta \in \mathfrak{G}_0$. Now, if $u = \sum_{i,\mu} a_i a^\mu (\sum_\lambda a^{n'\lambda} b_{i\mu\lambda})$ $= \sum_{i,\mu,\lambda} a_i a^\mu a^{n'\lambda} b_{i\mu\lambda}$ is an $\mathfrak{G}$-n.b.e. of A/B then every $b_{i\mu\lambda}$ is non-zero by Cor. 10.13, whence we see that every $\sum a^{n'\lambda} b_{i\mu\lambda}$ is a non-zero element of B_0. Hence, again by Cor. 10.13, u is an $\mathfrak{G}_0$-n.b.e. of A/B_0.

A subgroup S of a finite abelian group G is called a <u>correct subgroup</u> if G has a factorization $G = [g_1] \times \cdots \times [g_t]$ such that $S = [g_1^{\alpha_1}] \times \cdots \times [g_t^{\alpha_t}]$ with some α_i.

Lemma 10.15. <u>Let</u> G <u>be a</u> p-<u>primary abelian group of finite order</u>. <u>If a subgroup</u> S <u>of</u> G <u>contains</u> $G^p = \{g^p ; g \in G\}$ <u>then</u> S <u>is correct</u>.

<u>Proof</u>. Let G be of order p^e. The case $e = 1$ being trivial, we proceed with the induction relative to e. We assume $e > 1$ and $S \neq G$ or 1. As $S \supset G^p \supset S^p$, G^p is a correct subgroup of S by the induction hypothesis: $S = [s_1] \times \cdots \times [s_k]$ $(s_i \neq 1)$ and $T = G^p = [s_1^{\alpha_1}] \times \cdots \times [s_k^{\alpha_k}]$. Hence, by the relation $G^p \supset S^p$, we may set $\alpha_i = 1$ for $i < h$ and $\alpha_i = p$ for $i \geqslant h$. For every $i < h$, there exists $g_i \in G$ such that $s_i = g_i^p$. If $G^* = [g_1, \cdots, g_{h-1}, s_h, \cdots, s_k]$ then $G^* = [g_1] \times \cdots \times [g_{h-1}] \times [s_h] \times \cdots \times [s_k]$. In fact, $g_1^{\beta_1} \cdots g_{h-1}^{\beta_{k-1}} s_h^{\beta_k} \cdots s_k^{\beta_k} = 1$ implies $1 = s_1^{\beta_1} \cdots s_{h-1}^{\beta_{k-1}} (s_h^p)^{\beta_k} \cdots (s_k^p)^{\beta_k} \in T$, whence it follows $s_i^{\beta_i} = 1$ $(i < h)$, namely, $\beta_i = p\gamma_i$ $(i < h)$. We obtain therefore $1 = s_1^{\gamma_1} \cdots s_{h-1}^{\gamma_{k-1}} s_h^{\beta_k} \cdots s_k^{\beta_k}$

$\in S$, and eventually $g_1^{\beta_1} = s_1^{\gamma_1} = 1, \ldots, g_{h-1}^{\beta_{h-1}} = s_{h-1}^{\gamma_{h-1}} = 1, s_h^{\beta_h} = 1, \ldots, s_k^{\beta_k} = 1$. If $G = G^*$, our lemma is proved already. Otherwise, let g_o be in $G \backslash G^*$. Then $s = g_o^p \in T = [s_1] \times \ldots [s_{h-1}] \times [s_h^p] \times \ldots \times [s_k^p]$. Recalling that $s_i = g_i^p$ $(i < h)$, we obtain $s = t^p$ with some $t \in G^*$. Since $t \neq g_o$ and $(tg_o^{-1})^p = 1$, $g = tg_o^{-1}$ is of order p and $G^*[g] = G^* \times [g]$. If $G \neq G^* \times [g]$, an obvious induction completes the proof.

Theorem 10.16. Let A be a division ring. If A/B is an $\mathfrak{G}$-Kummer extension then it is completely basic, that is, any $\mathfrak{G}$-n.b.e. of A/B is an $\mathfrak{G}^*$-n.b.e. of $A/J(\mathfrak{G}^*)$ for every subgroup $\mathfrak{G}^*$ of $\mathfrak{G}$.

Proof. As is well-known, $\mathfrak{G} = \mathfrak{G}_1 \times \ldots \times \mathfrak{G}_t$ with the p_i-primary components $\mathfrak{G}_i$. If $\mathfrak{G}_o$ is a subgroup of $\mathfrak{G}$ with prime index p_1 then $\mathfrak{G}_o = \mathfrak{G}_1^* \times \mathfrak{G}_2^*$ with a subgroup $\mathfrak{G}_1^*$ and $\mathfrak{G}_2^* = \mathfrak{G}_2 \times \ldots \times \mathfrak{G}_t$. As $(\mathfrak{G}_1 : \mathfrak{G}_1^*) = p_1$ implies $\mathfrak{G}_1^* \supset \mathfrak{G}_1^{p_1}$, $\mathfrak{G}_1^*$ is a correct subgroup of $\mathfrak{G}_1$ (Lemma 10.15). Hence, by Lemma 10.14, we see that any $\mathfrak{G}$-n.b.e. of A/B is an $\mathfrak{G}_o$-n.b.e. of $A/J(\mathfrak{G}_o)$. Now, the proof of our theorem will be completed by the induction with respect to the order of $\mathfrak{G}$.

A central simple algebra of rank 4 over a field not of characteristic 2 is called a quaternion algebra, which may be characterized as in the next theorem.

Theorem 10.17. A is a quaternion algebra if and only if A/C is $\mathfrak{G}$-regular for some (abelian) $\mathfrak{G}$ of order 4.

Proof. By Lemma 10.3, it is left to prove the only if part. Assume that A be a quaternion algebra. If $A = (C)_2$ then $A = C[i, j]$ for $i = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ and $j = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, and there holds $ij = -ji$, $i^2 = 1$ and $j^2 = -1$. On the other hand, if A is a division ring then any maximal subfield M of A can be represented as $C[i]$ with some i such that $i^2 \in C$. Evidently, $\sigma : c_o + c_1 i$

$\longrightarrow c_o - c_1 i$ $(c_o, c_1 \in C)$ is a C-ring automorphism of M of order 2, and can be extended to an inner automorphism $\tilde{j}$ of A (Th. 4.6). Since $M|\tilde{j}^2 = 1$ and $i\tilde{j} = -i$, $A = C[i, j]$ and $j^2 \in V_A(M) \cap C[j] = C$. Thus, in either case, we have seen that there exist some $i, j \in A^*$ such that $A = C[i, j]$, $i^2 \in C$, $j^2 \in C$ and $ij = -ji$, and then $\mathfrak{G} = \{\tilde{1}, \tilde{i}, \tilde{j}, \tilde{ij}\}$ is a group of order 4 and $J(\mathfrak{G}) = C$.

If A is a quaternion division algebra then under the notation in the proof of Th. 10.17, $\mathfrak{G} = \{\tilde{1}, \tilde{i}\} \times \{\tilde{1}, \tilde{j}\}$ and A/C is an $\mathfrak{G}$-Kummer extension. However, $V_A(C) = A$ is not commutative, and hence $\mathfrak{G}(A/C) = \tilde{A}$ is not commutative by Cor. 9.5.

Nobusawa-Tominaga [1]; Ôhori-Tominaga [1].

11. Generating elements of Galois extensions

Throughout the present section, we assume again B is a simple ring. Concerning generating elements of a finite Galois extension A/B, there are a number of interesting results, and one will see that the tools used in the respective cases $[B:Z] = \infty$ and $[B:Z] < \infty$ are strikingly distinct. At first we shall dispose of the case $[B:Z] = \infty$. To this end, we shall consider the following properties:

(I) For every finitely generated right V-submodule N of A there exist a countably infinite number of elements $b_1, b_2, \cdots$, in B^* such that $\sum_1^\infty Nb_i = \oplus_1^\infty Nb_i$.

(I') For every finitely generated right Z-submodule N of A there exist a countably infinite number of elements $b_1, b_2, \cdots$, in B^* such that $\sum_1^\infty Nb_i = \oplus_1^\infty Nb_i$.

(II) For every B-B-submodule X of A left finite over B there exists an element x such that $X = BxB$.

If A/B possesses the property (II) and is left algebraic then for an arbitrary finite subset F of A we can find an element f such that $B[F] = B[f]$. In particular, if A/B is left algebraic (**resp**. left algebraic and of bounded degree) then A/B is left locally finite (resp. $[A:B]_L < \infty$), provided A/B possesses the property (II).

Proposition 11.1. *Let B be a division ring.*

(a) *If $[B:Z] = \infty$ then A/B possesses the property (I').*

(b) *If A is a division ring and $[B:Z] = \infty$ then A/B possesses the property (I).*

Proof. (a) Case I. B/Z is algebraic: Let M be a maximal subfield of B, that is obviously infinite and locally finite over Z (Th. 7.7). We set here $N = \oplus_1^s x_u Z$. We may assume then, without loss of generality, $\sum_1^s x_u M = \oplus_1^t x_u M$ $(t \leqq s)$, and we can find an intermediate field M_1 of M/Z finite over Z such that $N \subset \sum_1^t x_u M_1$. Choose arbitrarily an element $b \in M \setminus M_1$. If $\sum_1^t x_u y_u$

$= \sum_1^t x_u b y'_u$ for some y_u, y'_u in M_1 then $y_u = by'_u$, whence it follows $y_u = 0 = y'_u$. We have seen therefore $0 = \sum_1^t x_u M_1 \cap \sum_1^t x_u b M_1 \supset N \cap Nb$, so that $N + Nb = N \oplus Nb$. Assume now that we have found such non-zero elements $b_1, \ldots, b_q$ in B that $\sum_1^q Nb_i = \oplus_1^q Nb_i$. Then, we can apply the above argument for $N' = \sum_1^q Nb_i$ in place of N to obtain a non-zero element $b' \in B$ with $N' + N'b' = N' \oplus N'b'$. Setting $b_{q+1} = b_q b'$, we obtain $\sum_1^{q+1} Nb_i = \oplus_1^{q+1} Nb_i$, which completes the induction.

Case II. B/Z is not algebraic: There exists an element x in B that is transcendental over Z. If $F_i (\subset B)$ is the quotient field of $Z[x^{2^i}]$ $(i = 0, 1, \ldots)$, then $F_0 \supset F_1 \supset \ldots (\supset Z)$. We set here $N = \oplus_1^s x_u Z$ and $n(i) = [\sum_1^s x_u F_i : F_i]_R$ $(\leqslant s)$, and we shall prove that $\max n(i) = s$. Suppose on the contrary $\max n(i) = n(p) = s' < s$. Then, without loss of generality, we may assume that $\sum_1^s x_u F_p = \oplus_1^{s'} x_u F_p$, so that $x_{s'+1} = \sum_1^{s'} x_u f_u$ with some f_u in F_p. Since $\{x_1, \ldots, x_s\}$ is free over Z, some one of f_u's, say f_1, is not contained in Z. We set $f_1 = (\sum_0^m y^j z_j)^{-1}(\sum_0^m y^j z'_j)$ $(y = x^{2^p}$ and $z_j, z'_j \in Z)$, and choose a positive integer t such that $2^t > m$. As $F_p \supset F_{p+t}$ and the maximality of $n(p)$ imply $n(p+t) = n(p)$, there holds $\sum_1^s x_u F_{p+t} = \oplus_1^{s'} x_u F_{p+t}$, whence it follows that f_1 is contained in F_{p+t}. Accordingly, noting that $\{1, y, \ldots, y^{2^t-1}\}$ is linearly independent over F_{p+t}, $\sum_0^m y^j z'_j = (\sum_0^m y^j z_j) f_1$ yields $z'_j = z_j f_1$ $(0 \leqslant j \leqslant m)$. Since some of z_j's is non-zero, we obtain a contradiction $f_1 \in Z$. Hence, we have seen $n(p) = s$, namely, $\sum_1^s x_u F_p = \oplus_1^s x_u F_p$. Now, noting that the subset $\{b_k = y^{k-1}$; $k = 1, 2, \ldots\}$ of F_p is free over Z, it is easy to see that

$\sum_1^\infty Nb_k = \bigoplus_1^s x_u(\bigoplus_1^\infty b_k Z) = \bigoplus_1^\infty Nb_k$, which is our assertion.

(b) The proof will be completed by a slight modification of that of (a). In case B/Z is algebraic, take a maximal subfield M of B. Then $M \cdot V = M \otimes_Z V$ is a division ring that is locally finite and infinite over V. Hence, in Case I of the proof of (a), we can replace Z and M by V and $M \cdot V$, respectively. On the other hand, assume that B contains an element x that is transcendental over Z. Then, $\{x^j\}$ is free over V, and so the division subring F_i generated by $V[x^{2^i}]$ is a quotient division ring of the polynomial domain $V[x^{2^i}]$. Hence, in Case II of the proof of (a), we can replace Z by V.

Lemma 11.2. *Let A be Galois over a division ring B, and $B \cdot V$-A-irreducible. Let X be a B-B-submodule of A left finite over B. If x is an arbitrary element of X, $x\mathfrak{o}V_R$ possesses a right V-basis and $[x\mathfrak{o}V_R : V]_R = [BxB : B]_L$. In particular, if x is an element of X such that $[x\mathfrak{o}V_R : V]_R = [X : B]_L$ then $X = BxB$.*

Proof. The mapping $BxB \mid \alpha \longrightarrow x\alpha$ $(\alpha \in \mathfrak{o}V_R)$ defines a V_R-isomorphism of $BxB \mid \mathfrak{o}V_R$ onto $x\mathfrak{o}V_R$. Accordingly, it follows $[BxB : B]_L = [(BxB \mid \mathfrak{o})V_R : V_R]_R = [x\mathfrak{o}V_R : V]_R$ by Lemma 5.8 (a).

Proposition 11.3. *Let B be a division ring. If A is Galois over B and $B \cdot V$-A-irreducible, then (I) implies (II).*

Proof. Let $X = Bx_1 + \ldots + Bx_m$. Then $N = \sum_1^m x_i \mathfrak{o}V_R$ is a finitely generated right V-submodule of A (Lemma 11.2). Hence, by the property (I), there exist a countably infinite number of non-zero elements $b_1, b_2, \ldots$ in B such that $\sum_1^\infty Nb_i = \bigoplus_1^\infty Nb_i$. If we set $x = \sum_1^m x_i b_i$ $(\in X)$, then one will easily see that $X \mid \alpha \longrightarrow x\alpha$ $(\alpha \in \mathfrak{o}V_R)$ is a V-isomorphism. It follows therefore $[x\mathfrak{o}V_R : V]_R = [(X \mid \mathfrak{o})V_R : V_R]_R = [X : B]_L$ (Lemma 5.8 (a)). Now, by Lemma 11.2, we obtain $X = BxB$.

Combining Prop. 11.1 (b) with Prop. 11.3, we obtain the next:

Corollary 11.4. *Let a division ring A be Galois over B, and $[B : Z] = \infty$.*

(a) For every B-B-submodule X of A left finite over B there exists an element x such that X = BxB. In particular, every intermediate ring T of A/B left finite over B is singly generated over B, namely, T = B[t] for some t.

(b) If A/B is left algebraic then A/B is left locally finite.

(c) If A/B is left algebraic and of bounded degree then $[A:B] < \infty$.

Theorem 11.5. Assume that $\mathcal{G}A_R$ is dense in $V_\sigma(B_L)$ and $[B:Z] = \infty$.

(a) If A/B is left algebraic then it is left locally finite.

(b) If A/B is left algebraic and of bounded degree then $[A:B]_L < \infty$.

Proof. By Cor. 8.5, there exists some $B' = \sum_1^n D'e'_{ij} \in \mathfrak{L}^\circ_{l.f}$ such that $V_A(\{e'_{ij}\})/D'$ is left algebraic (and of bounded degree in (b)). Since $J(\mathcal{G}(B')) = B'$ by Prop. 6.11, $V_A(\{e'_{ij}\})$ is Galois over the division ring D' with $[D':V_{D'}(D')] = \infty$ (Cor. 7.11). Hence, by Cor. 11.4 (b), $V_A(\{e'_{ij}\})/D'$ is left locally finite. Accordingly, A/B' and hence A/B is left locally finite. Similarly, (b) is a consequence of Cor. 11.4 (c).

Lemma 11.6. Assume that A/B is h-Galois. Let T be in $\mathfrak{L}^\circ_{l.f}/\Gamma$, and $W = T \wedge U$, where $U = V_V(\Gamma)$. If a subset of T is right free over W, then so is over U.

Proof. Since $J(\mathcal{G}(T)) = T$ by Prop. 6.11, $U|\mathcal{G}(T)$ is a Galois group of U/W. Now, assume that $\{t_1, \ldots, t_m\}$ is a subset of T that is not right free over U. Then, without loss of generality, we may assume that $t_1 = \sum_2^m t_j u_j$ $(u_j \in U)$ is a non-trivial relation of the shortest length. Since $0 = t_1 - t_1\sigma = \sum_2^m t_j(u_j - u_j\sigma)$ for every σ in $\mathcal{G}(T)$, it follows then $u_2, \ldots, u_m \in W$, namely, $\{t_1, \ldots, t_m\}$ is not right free over W.

Now, we are at the position to prove the first principal theorem.

Theorem 11.7. Let A/B be h-Galois, and $[B:Z] = \infty$. If A/B is left algebraic then for every B-B-submodule X of A left finite over B there exists an element x such that X = BxB, in particular,

for an arbitrary finite subset F of A the subring B[F] is singly generated over B.

Proof. By Th. 11.5, A/B is left locally finite. Hence, A is B·V-A-irreducible (Th. 6.1). Then, taking the validity of Cor. 5.6 (b) into the mind, we may assume from the beginning that B is a division ring. Now, let N be a finitely generated right V-submodule of A, and $U = V_V(\Gamma)$. Then, $N = \oplus_1^m t_j U$. Take an arbitrary T in $\mathfrak{L}^{\circ}_{1.f}/\{\Gamma, t_1, \cdots, t_m\}$, and set $W = T \cap U$ and $N' = \oplus_1^m t_j W$. Obviously, $[W:Z] \leqq [V_T(B):Z] \leqq [T:B]_L < \infty$ (Prop. 4.2). Accordingly, by Prop. 11.1 (a), there exist a countably infinite number of non-zero elements $b_1, b_2, \cdots$ in B such that $\sum_1^{\infty} N'b_i = \oplus_1^{\infty} N'b_i = \oplus_{i,j} t_j b_i W$. Recalling that every $t_j b_i$ is contained in T, Lemma 11.6 implies that $\sum_{i,j} t_j b_i U = \oplus_{i,j} t_j b_i U = \oplus_i Nb_i$. We have seen thus A/B has the property (I). Now, our assertion is clear by Prop. 11.3.

Corollary 11.8. Assume that A is Galois and finite over B and $[B:Z] = \infty$.

(a) If X is an arbitrary B-B-submodule of A then $X = BxB$ for some x. In particular, every intermediate ring of A/B is singly generated over B.

(b) If A' is an intermediate ring of A/B·V then $A' = B[a']$ with some unit a'. In particular, $A = B[a]$ with some unit a.

(c) If V is a division ring, then for every intermediate ring A' of A/B there exists a unit a' of A' such that $A' = B[a']$.

Proof. We shall prove here (b) and (c).

(b) As $B \cdot V = B \otimes_Z V$ is simple and $V_A(B \cdot V) = C_o$, A' is a simple ring by Th. 7.2 and Prop. 7.3 (b). Accordingly, we have $A' = \sum_1^{n'} D'e'_{ij}$ where $E' = \{e'_{ij}\}$ is a system of matrix units such that $V_{A'}(E')$ is the division ring D'. Obviously, by (a), it suffices to prove the case $n' > 1$. Moreover, in virtue of Prop. 8.3 (a), we may assume that B contains an element $b = \sum x'_{ij} e'_{ij}$ $(x'_{ij} \in D')$ such as $x'_{1n} = 1$ and $x'_{in} = 0$ for every $i > 1$. We consider here the

simple ring $B_1 = B[E'] = \sum_1^{n'} D_1 e'_{ij}$, where $D_1 = V_{B_1}(E')$ is a division subring of D'. We may assume further E' contains Γ. It follows then $V_A(B_1) = V_V(E') = V_U(E')$ is a division ring, and therefore $V_A(E')$ is Galois and finite over D_1 by Th. 7.2. Since D_1 is infinite over its center (Cor. 7.11), we can find a non-zero element d' such that $D' = D_1[d']$ (by (a)). Setting $a' = 1 - (d'e'_{21} + \sum_3^{n'} e'_{ii-1})$, a' is a unit of A' and Lemma 8.4 (b) proves $A' = B[b,\ d'e'_{21} + \sum_3^{n'} e'_{ii-1}] = B[a']$.

(b) As V is a division ring, A' is simple by Prop. 7.3 (b) and the proof proceeds in the same way as in (b).

Concerning the case $[B:Z] < \infty$, as one will see soon later, a number of important results will be given as consequences of an efficient proposition.

Lemma 11.9. *Let A be a division ring with $[A:C] = t^2$, and M a maximal subfield of A. If $M = C[m]$ then there exists an element a such that $A = \bigoplus_{i,j=0}^{t-1} m^i a m^j C$.*

Proof. Since $\tilde{M}$ is abelian and $\tilde{M}\cdot M_R = M_L \cdot M_R$, A is $M_L \cdot M_R$-isomorphic to $M_L \cdot M_R = \sum_{i,j=0}^{t-1} m_L^i m_R^j C_R$ (Th. 9.1). If $a \longleftrightarrow 1$ under the above isomorphism then it is obvious that a is the element requested.

Theorem 11.10. *If A is a separable simple algebra of finite rank over a field Φ then $A = \Phi[u, u\tilde{r}]$ with some $u, r \in A^*$.*

Proof. Case I. $n = |A| = 1$: A contains a separable maximal subfield M over C (Cor. 7.9). Since $M = \Phi[u]$ with some $u \in M^*$, there exists an element $r \in A^*$ such that $A = \bigoplus_{i,j} u^i r u^j C = \sum_{i,j} u^i (u\tilde{r})^j C = \Phi[u, u\tilde{r}]$ (Lemma 11.9).

Case II. $n > 1$: As D is a separable division algebra over Φ, by Case I there exist $x, d \in D^*$ such that $D = \Phi[x, x\tilde{d}]$. We set $t = \sum_1^n e_{in-i+1}$ $(= t^{-1})$, $u^* = \sum_2^n e_{ii-1}$ and $v^* = u^*\tilde{t} = \sum_2^n e_{i-1i}$. Then, one will easily see that $e_{ij} = u^{*i-1} v^{*n-1} u^{*n-1} v^{*j-1}$

$(i, j = 1, \ldots, n)$. In case $D = \Phi$, $\Phi[1 - u^*, (1 - u^*)\tilde{t}] = \Phi[u^*, v^*] = \Phi[E] = A$ and $1 - u^* \in A^*$. Thus, in what follows, we may restrict our attention to the case $D \neq \Phi$. Under this situation, if $x\tilde{d}\cdot x = 1$, or $x\tilde{d} = x^{-1}$, then $\Phi[x, x\tilde{d}] = \Phi[x]$ and $x^2 \neq 1$. Accordingly, we may assume further that $x\tilde{d}\cdot x \neq 1$. If $u = u^* + xe_{1n}$ and $v = u\tilde{dt} = v^* + x\tilde{d}\cdot e_{n1}$ then $u^{-1} = v^* + x^{-1}e_{n1} \in \Phi[u]$ yields $(x^{-1} - xd)e_{n1} = u^{-1} - v \in \Phi[u, v]$, whence it follows $(1 - xd\cdot x)e_{nn} = (u^{-1} - v)u \in \Phi[u, v]$. Noting that $x = u^n$ and $xd = v^n$ are contained in $\Phi[u, v]$, we obtain $e_{nn} \in \Phi[u, v]$, which forces $e_{ij} = v^{n-i}e_{nn}u^{n-j} \in \Phi[u, v]$. Consequently, we have $\Phi[u, v] = \Phi[x, x\tilde{d}, E] = A$, completing the proof.

Corollary 11.11. *Let A be a simple algebra over a perfect field Φ. If A/Φ is 3-algebraic then it is locally finite. If $n > 1$ and A/Φ is 2-algebraic then it is locally finite.*

Proof. First, assume that A is a division ring and 3-algebraic over Φ. If a_1, a_2, a_3 are in A then $\Phi[a_1, a_2, a_3] = \Phi[a_1', a_2']$ with some a_1', a_2' (Th. 11.10). Hence, an easy induction will prove that A/Φ is locally finite. Next, assume that $n > 1$ and A/Φ is 2-algebraic. Let d_1, d_2, d_3 be non-zero elements of D. If $a_1 = \sum x_{ij}e_{ij}$ where $x_{11} = d_1$, $x_{21} = d_2$, $x_{1n} = 1$ and each of other x_{ij}'s is 0, and $a_2 = d_3e_{21} + \sum_3^n e_{ii-1}$, then $\Phi[a_1, a_2]$ is finite over Φ and contains all d_i's (Lemma 8.4 (b)), which means that D/Φ is 3-algebraic. Hence, A/Φ is locally finite by the first assertion proved above.

Corollary 11.12. *If A is finite Galois over B and $[B:Z] < \infty$ then $A = (B \cap C)[u, u\tilde{r}]$ for some $u, r \in A^*$.*

Proof. Since $[A:C] < \infty$ by Cor. 7.11 and C is finite Galois over $B \cap C$, A is separable and of finite rank over $B \cap C$. Hence, our assertion is obvious by Th. 11.10.

Corollary 11.13. Let A be a separable division algebra of finite rank over a field Φ. If a is an element of A not contained in C then $A = \Phi[a, a']$ for some a'.

Proof. Let T be an arbitrary intermediate ring of A/Φ properly contained in A, and y an element of $A \setminus T$ such that $ay \neq ya$. Now, suppose that there exist different elements $c_1, c_2, c_3 \in \Phi$ such that $a_i = (y + c_i)a(y + c_i)^{-1}$ are contained in T $(i = 1, 2, 3)$. Then, $(y + c_i)a = a_i(y + c_i)$ $(i = 1, 2, 3)$ yield $(c_i - c_j)a = (a_i - a_j)y + (a_ic_i - a_jc_j)$ $(i, j = 1, 2, 3)$. From these, we readily obtain $\{(c_1 - c_3)(a_1 - a_2) - (c_1 - c_2)(a_1 - a_3)\}y + (c_1 - c_3)(a_1c_1 - a_2c_2) - (c_1 - c_2)(a_1c_1 - a_3c_3) = 0$, or equivalently, $(c_1 - c_3)(a_1 - a_2) - (c_1 - c_2)(a_1 - a_3) = 0$ and $(c_1 - c_3)(a_1c_1 - a_2c_2) - (c_1 - c_2)(a_1c_1 - a_3c_3) = 0$. Subtracting the latter from the former multiplied by c_1, it follows $(c_1 - c_3)\{(c_2 - c_1)a_2 + (c_1 - c_2)a_3\} = 0$, whence $a_2 = a_3$. We have then $(c_2 - c_3)a = a_2(c_2 - c_3)$, so that $a = a_2$ and $(y + c_2)a = a(y + c_2)$, which yields a contradiction $ya = ay$. We have seen thus there exist at most two c's in Φ such that $(y + c)a(y + c)^{-1} \in T$. By the light of this remark, we can prove our corollary. As was shown in the proof of Th. 11.10, there exist some u, v such that $M = \Phi[u]$ is a maximal subfield of A and $A = \Phi[u, y]$. Since there are only a finite number of intermediate fields of M/C, the number of intermediate rings of A/M is finite, too (Th. 7.7). Now, let $\{ T_1, \ldots, T_q \}$ be the set of all the intermediate rings of A/M different from A. Then, v is not contained in any T_i. We may assume here that $va \neq av$. In fact, if $av = va$ then $a(u + v) \neq (u + v)a$ by $a \notin C$, and then $A = \Phi[u, u + v]$ enables us to see that $u + v$ can replace v. Under this situation, for every i there exist at most two c's in Φ such that $(v + c)a(v + c)^{-1} \in T_i$. As Φ is infinite by $A \neq C$, we can find then an element $v_o = v + c_o$ $(c_o \in \Phi)$ such that $a\tilde{v}_o \notin T_i$ for

all i. Accordingly, it follows $A = M[a\tilde{v}_o] = \Phi[a\tilde{v}_o, u] = \Phi[a, u\tilde{v}_o^{-1}]$.

Lemma 11.14. *Let* A *be finite Galois over* B *with* $[B:Z] < \infty$, *and* A^* *a simple intermediate ring of* A/B *with the center* C^* *contained in* C_o. *Let* $\Phi = B \cap C$, *and* $A^* = \sum_1^{n^*} D^* e_{ij}^*$ *where* $E^* = \{ e_{ij}^* \}$ *is a system of matrix units and* $D^* = V_{A^*}(E^*)$ *a division ring*.

(a) $Z \cdot C^* = Z[c_o]$ *for some non-zero* $c_o \in A^* \cap C$.

(b) *If* x *is an element of* D^* *not contained in* C^* *and* $Z \cdot C^* = Z[c_o]$ *with some* $c_o \in A^* \cap C$ *then there exists a non-zero element* $y \in D^*$ *such that* $D^* = C^*[x, y]$ *and* $\Phi[y]$ *contains* c_o.

Proof. (a) Since $[A:C] < \infty$ (Cor. 7.11), $B \cdot C = B \otimes_Z Z \cdot C$ is simple and $V_A(H) = V_A(B \cdot C)$, we see that $H = B \cdot C$ (Th. 7.7). Accordingly, $C_o = Z \cdot C$. Noting that C is a finite Galois extension field over Φ with the Galois group $C \mid \mathfrak{G}$, we see that $\mathfrak{G}(C_o/Z) \simeq \mathfrak{G}(C/\Phi)$ by the contraction. Hence, the intermediate field $Z \cdot C^*$ of C_o/Z is represented as $Z \cdot C'$ with some intermediate field C' of C/Φ. Since $C' = \Phi[c_o]$ with some non-zero $c_o \in A^* \cap C$, it follows $Z \cdot C^* = Z \cdot C' = Z[c_o]$.

(b) Since $[D^*:C^*] < \infty$ (Cor. 7.11), there exists an element y' in D^* such that $D^* = C^*[x, y']$ (Cor. 11.13). Obviously, c_o is separable over Φ and the field $\Phi[c_o, y']$ is finite over Φ, and so $\Phi[c_o, y'] = \Phi[y]$ with some y. Consequently, $C^*[x, y] = C^*[x, y', c_o] = D^*$.

We can prove now the following efficient proposition.

Proposition 11.15. *Let* A *be finite Galois over* B *with* $[B:Z] < \infty$, *and* A^* *a simple intermediate ring of* A/B *such that the center* C^* *of* A^* *is contained in* C_o.

(a) *If* A^* *is commutative then* $A^* = Z[c_o]$ *with some* c_o.

(b) *If* a *is an element of* A^* *not contained in* C^* *then there exists a unit* a' *such that* $A^* = Z[a, a']$.

Proof. (a) is evident by Lemma 11.14 (a). To prove (b), we set $\Phi = B \cap C$ and $A^* = \sum_1^{n^*} D^* e^*_{ij}$, where $E^* = \{ e^*_{ij} \}$ is a system of matrix units and $D^* = V_{A^*}(E^*)$ a division ring. Then, $[A: \Phi] < \infty$ by Cor. 7.11. Again by Lemma 11.14 (a), there exists a non-zero $c_o \in A^* \cap C$ such that $Z \cdot C^* = Z[c_o]$, and hence all the assumptions in Prop. 8.7 are fulfilled provided $n^* \geqslant 2$. If $n^* = 1$, there exists some $a' \in D^*$ such that $D^* = C^*[a, a']$ and $\Phi[a'] \ni c_o$ (Lemma 11.14 (b)), and so $Z[a, a'] = Z[a, a', c_o] = (Z \cdot C^*)[a, a'] = D^* = A^*$. Thus, in what follows, we may restrict our attention to the case $n^* \geqslant 2$. In general, if r is a unit of A^* then the centers of $B\tilde{r}$ and $V_A(B\tilde{r})$ coincide with $Z\tilde{r}$ and $C_o\tilde{r}$ respectively, A is finite Galois over $B\tilde{r}$, $B\tilde{r} \cap C = \Phi$, $(Z\tilde{r}) \cdot C^* = (Z\tilde{r})[c_o]$ and $[B\tilde{r}: Z\tilde{r}] < \infty$. Hence, all the assumptions attached to A/B and A^* by now are preserved for $A/B\tilde{r}$ and A^*. In below, the remark will be used often without mention. We shall distinguish here between three cases.

Case I. $D^* = C^*$: There exists a unit $r \in A^*$ such that $a\tilde{r} = \sum_1^{n^*} x_{ij} e^*_{ij}$ with $x_{1n^*} = c_o$ and $x_{in^*} = 0$ for every $i \geqslant 2$ (Prop. 8.3 (a)). Hence, there exists a unit $a'' \in A^*$ such that $A^* = (Z\tilde{r})[a\tilde{r}, a''] = Z[a, a''\tilde{r}^{-1}]$ (Prop. 8.7 (a)).

Case II. $D^* \supsetneqq C^*$ and $n^* > 2$: For an arbitrary element x in $D^* \backslash C^*$ we can find a non-zero element y such that $D^* = C[x, y]$ and $\Phi[y] \ni c_o$ (Lemma 11.14 (b)). Since we can find a unit r in A^* such that $a\tilde{r} = \sum_1^{n^*} x_{ij} e^*_{ij}$ with $x_{1n^*} = x$, $x_{1n^*-1} = y$ and $x_{in^*} = 0$ for every $i \geqslant 2$ (Prop. 8.3 (b)), again by Prop. 8.7 (a) there exists a unit a'' of A^* such that $A^* = (Z\tilde{r})[a\tilde{r}, a''] = Z[a, a''\tilde{r}^{-1}]$.

Case III. $D^* \supsetneqq C^*$ and $n^* = 2$: Again by Prop. 8.3 (a) there exists a unit r of A^* such that $a\tilde{r} = de^*_{11} + d'e^*_{21} + e^*_{12}$ ($d, d' \in D^*$). If $\{ d, d' \} \not\subset C^*$ then we can find some non-zero $y \in D^*$ such that $D^* = C^*[y, d, d']$ and $\Phi[y] \ni c_o$ (Lemma 11.14 (b)), and then $A^* = (Z\tilde{r})[a\tilde{r}, ye^*_{21}] = Z[a, (ye^*_{21})\tilde{r}^{-1}]$ by Prop. 8.7 (b). While, if $\{ d, d' \} \subset C^*$, in any rate, there exist non-zero elements x, y in D^* such that $D^* = C^*[x, y]$ and $\Phi[y] \ni c_o$ (Lemma 11.14 (b)).

We consider here the polynomial $f(\lambda) = \lambda^2 - d\lambda - d'$ in $C^*[\lambda]$. If $z = y^{-1}x$ and $z + y^{-1}$ are roots of $f(\lambda)$ in D^* then by a brief computation we see that $f(z + \beta y^{-1}) = f(z + y^{-1}) + (\beta - 1)\{f(z + y^{-1}) - f(z)\} + \beta(\beta - 1)y^{-2} = \beta(\beta - 1)y^{-2}$ for every $\beta \in \Phi$. Recalling here that $[A:\Phi] < \infty$ and $D^* \supsetneqq C^*$, Φ is evidently an infinite field. Accordingly, we can find some $\gamma \in \Phi$ such that $f(y^{-1}(x + \gamma)) = f(z + \gamma y^{-1}) \neq 0$. We may assume thus from the beginning that $f(y^{-1}x) \neq 0$, and then it follows $A^* = (Z\tilde{r})[a\tilde{r}, xe^*_{21} + ye^*_{22}] = Z[a, (xe^*_{21} + ye^*_{22})\tilde{r}^{-1}]$ (Prop. 8.7 (c)). We have seen thus in either case $A^* = Z[a, a"]$ with some $a"$. Noting again is infinite, one will easily see that there exists an element $\alpha \in \Phi$ such that $a' = a" - \alpha$ is a unit of A^*. Then, we obtain $A^* = Z[a, a"] = Z[a, a']$.

Combining Cor. 11.8 (b) with Prop. 11.15 and Cor. 11.12, one will readily see the following:

Theorem 11.16. *Let A be finite Galois over B.*

(a) *If a is an element of A not contained in C then there exists a unit a' such that $A = B[a, a']$. Accordingly, A/B is singly generated if and only if $A = C$ or $B \not\subset C$.*

(b) *$A = B[u, u\tilde{r}]$ with some $u, r \in A^\cdot$.*

Corollary 11.17. *Let A be left algebraic over B.*

(a) *In order that $[A:C] < \infty$, it is necessary and sufficient that $[V:C] < \infty$ and $[B:Z] < \infty$.*

(b) *If $[A:C] < \infty$ then A/B is locally finite.*

Proof. (a) By Cor. 7.11, it suffices to prove the sufficiency. There exists some $B' = \sum_1^n D'e'_{ij} \in \mathfrak{R}^{\circ}_{l.f}$ such that $V_A(\{e'_{ij}\})$ is left algebraic over D' (Cor. 8.5). Since $[B':V_{B'}(B')] < \infty$ again by Cor. 7.11, we may assume from the beginning that A is a division ring. Then, noting that $B\cdot C = B \otimes_Z Z\cdot C$, there holds $[B\cdot C:C] = [B\cdot C:Z\cdot C]\cdot[Z\cdot C:C] \leqq [B:Z]\cdot[V:C] < \infty$. Hence, $B\cdot C = V_A^2(B\cdot C) = V_A(V)$, and so $[A:C] = [A:B\cdot C]\cdot[B\cdot C:C] = [V:C]\cdot[B\cdot C:C] < \infty$ (Th. 7.7).

(b) In case B is contained in C, our assertion can be seen by a direct computation. In what follows, we shall assume that $B \not\subset C$. Then, by Th. 11.16 (a), there exists an element a such that $A = (B\cdot C)[a]$. Now, let F be an arbitrary finite subset of A. Then, C contains a finite subset F' such that $B[F] \subset B[F', a] = B[a]\cdot B[F']$. Since we can easily see $[B[F']:B]_L < \infty$, our assertion is a consequence of (a) and Cor. 7.12.

The next contains obviously Cor. 11.17 (b).

Theorem 11.18. Let A be left algebraic over B, and $[B:Z] < \infty$. In order that A/B be locally finite, it is necessary and sufficient that $A/B\cdot C$ be left locally finite.

Proof. It remains only to prove the sufficiency. At first we shall prove our assertion for the case that B is a regular subring. Since $B\cdot C = B \otimes_Z Z\cdot C$, $Z\cdot C$ is a subfield of C_o and $B\cdot C$ is a simple ring with $[B\cdot C:Z\cdot C] = [B:Z] < \infty$. Now, let F be an arbitrary finite subset of A. Then, $A' = (B\cdot C)[E, F]$ is a simple ring with $[A':B\cdot C]_L < \infty$, and so $[A':V_{A'}(A')] < \infty$ by Cor. 7.11. Hence, A'/B is locally finite by Cor. 11.17 (b), which means evidently the local finiteness of A/B. Next, we shall prove the general case. By Cor. 8.5 and Prop. 7.12 there exists some $B' = \sum_1^n D'e'_{ij} \in \mathfrak{L}^{\circ}_{l.f} \cap \mathfrak{L}^{\circ}_{r.f}$ such that $V_A(\{e'_{ij}\})$ is left algebraic over D'. Since $B'\cdot C = \sum_1^n (D'\cdot C)e'_{ij}$ is left finite over $B\cdot C$, $A/B'\cdot C$ is left locally finite, or what is the same, $V_A(\{e'_{ij}\})/D'\cdot C$ is left locally finite. Hence, noting that $[D':V_{D'}(D')] \leqq [B':V_{B'}(B')] < \infty$ (Cor. 7.11), the first step proves that $V_A(\{e'_{ij}\})/D'$ is locally finite, or equivalently, A/B' is locally finite. Consequently, it follows that A/B is locally finite.

Albert [1], [2]; Faith [5]; Inatomi [1]; Jacobson [7]; Kasch [1], [2]; Kasch-Tominaga [1]; Moriya-Nagahara [1]; Nagahara [1], [2], [3], [4], [5], [7]; Nagahara-Tominaga [6], [7], [12], Nagahara-Nakajima-Tominaga [1].

12. Generating elements of Galois extensions (Continued)

As applications of Prop. 11.15, we can prove a number of interesting theorems. The first one is the following extension of Cor. 11.13.

Theorem 12.1. Let A be a separable simple algebra of finite rank over a field Φ. If a is an element of A not contained in C then $A = \Phi[a, a']$ with some $a' \in A^{\cdot}$.

Proof. By Cor. 7.9 and Th. 4.6 (a), we can easily see that there exists a finite Galois extension field C^* over Φ such that $A^* = A \otimes_C C^*$ coincides with $(C^*)_m$. Then, A^* is finite Galois over Φ, and so we can apply Prop. 11.15 to A^*/Φ and A to see that there exists a unit a' such that $A = \Phi[a, a']$.

The next is equivalent to Th. 12.1.

Theorem 12.2. Let A be a central simple algebra of finite rank over C, and T a unital subring of A such that $T \cap C$ is a field and C is finite and separable over $T \cap C$. If A is commutative or $T \not\subset C$ then $A = T[a]$ with some $a \in A^{\cdot}$, and conversely.

Corollary 12.3. Let A be Galois and finite over B of characteristic 0, and T a simple intermediate ring of A/B. In order that T/B be singly generated, it is necessary and sufficient that either T be commutative or $B \not\subset V_T(T)$.

Proof. By the validity of Cor. 11.8, it suffices to prove the case $[B:Z] < \infty$. As $[A:B \cap C] = [A:C] \cdot [C:B \cap C] < \infty$ by Cor. 7.11, T is a separable simple algebra of finite rank over $B \cap C$. Hence, our assertion is a direct consequence of Th. 12.2.

The rest of the present section will be devoted exclusively to the study on generating elements of intermediate rings of a finite Galois extension. We shall prove now the following useful theorem.

Theorem 12.4. Let A be Galois and finite over B. If V is commutative then for each intermediate ring T of A/B there exists a unit t of T such that $T = B[t]$.

Proof. It suffices to prove the case $[B:Z] < \infty$ (Cor. 11.8 (c)). Since T is a simple ring (Prop. 7.3 (b)) and $V_A(T) \subset V = C_o$, if

B is not contained in the center C' of T then for an arbitrary element $b \in B \backslash C'$ we can find a unit t such that $T = Z[b, t] = B[t]$ (Prop. 11.15). On the other hand, if B is contained in C' then V/B is Galois. Hence, the field $T = V_T(B)$ is separable over B, and so singly generated over B.

Now, we shall prove an extension of the latter part of Th. 11.16 (a), that will be given after the following lemma.

Lemma 12.5. *Let A be finite Galois over B, and $B \neq Z$. Let T be an intermediate ring of A/B. If $T \subset H$ or $T \supset V$ then T is singly generated over B.*

Proof. If $T \subset H$, our assertion is contained in Th. 12.4. Thus, taking Cor. 11.8 into our consideration, we may assume that $T \supset V$ and $[B:Z] < \infty$. Since $B \cdot V = B \otimes_Z V$ is a simple ring and $V_A(B \cdot V)$ is the field C_o, A is finite Galois over $B \cdot V$ (Th. 7.2) and T is a simple ring such that $V_A(T) \subset V_A(B \cdot V) = C_o$ (Prop. 7.3 (b)). If b is an arbitrary element of B Z then b is in $T \backslash V_T(T)$ of course, and hence we can find an element t such that $T = Z[b, t] = B[t]$ (Prop. 11.15).

Theorem 12.6. *Let A be finite Galois over B, and T a simple intermediate ring of A/B such that $\tilde{T}V \subset T$. If T is commutative or B is not contained in the center of T then T/B is singly generated, and conversely.*

Proof. Again by Cor. 11.8, it suffices to consider the case $[B:Z] < \infty$. If C is finite then so is T by $[A:C] < \infty$ (Cor. 7.11), and so T is a separable simple algebra of finite rank over $B \cap V_T(T)$. Hence, T/B is singly generated by Th. 12.2. In what follows, we may assume therefore that C is infinite. Then, $V \subset T$ or $T \subset H$ (Prop. 8.10 (a)) and our assertion for the case $B \neq Z$ has been shown in Lemma 12.5. Hence, we may assume further that $B = Z$. Now, $B = Z \subset C_o$ implies $V_A(C_o) = V$, and hence H coincides with the field C_o (Th. 7.7). If T is commutative then $T \subset H$ in any rate (even when $V \subset T$) and T/B is singly generated by Th. 12.4. On the other hand, if $B \not\subset V_T(T)$ then $V \subset T$, for

$T \subset H = C_o$ implies $B \subset T = V_T(T)$. Hence $V_A(T) \subset H = C_o$, which enables us to apply Prop. 11.15 to A/B and T. Accordingly, if b is an arbitrary element of $B \setminus V_T(T)$ then there exists an element t with $T = Z[b, t] = B[t]$.

Corollary 12.7. Let A be Galois and finite over B. If T is a simple intermediate ring of A/B such that $\widetilde{TV} \subset T$ then $T = B[t, t\widetilde{r}]$ for some $t \in T$ and $r \in T^*$.

Proof. By the light of Th. 12.6, it suffices to prove the case $B \subset V_T(T)$. If C is finite then T is a separable simple algebra of finite rank over B by $[A:C] < \infty$ (Cor. 7.11), so that our assertion is clear by Th. 11.10. On the other hand, if C is infinite then $T \subset H$ or $T \supset V \supset V_A(V_T(T)) \supset T$, namely, $T = V$ (Prop. 8.10 (a)). Hence, this time, our assertion is a consequence of Ths. 12.4 and 11.16 (b).

Lemma 12.8. Let A be finite Galois over B, and V a division ring. If $T_1 \supset T_2$ are intermediate rings of A/B then $[T_1:V_{T_1}(Z)] \geqslant [T_2:V_{T_2}(Z)]$.

Proof. At first, one may recall that every intermediate ring of A/B is simple (Prop. 7.3 (b)). If K_i is the center of T_i then $\infty > [V:B \cap C] \geqslant [K_i \cdot Z:K_i] = [T_i:V_{T_i}(Z)]$ (Th. 7.7). Now, we can find a subset $\{z_1, \cdots, z_t\}$ of Z as a K_2-basis of $K_2 \cdot Z$. If $\{z_1, \cdots, z_t\}$ is not free over $V_A(T_2)$ then, without loss of generality, we may assume that $z_1 = \sum_2^s z_i v_i$ ($v_i \in V_A(T_2)$, $2 \leqslant s \leqslant t$) is a non-trivial relation of the shortest length. For every σ in $\mathfrak{G}(T_2)$, we have then $\sum_2^s z_i v_i = z_1 = z_1\sigma = \sum_2^s z_i(v_i\sigma)$. Since every $v_i\sigma$ is in $V_A(T_2)$, it follows $v_i\sigma = v_i$ ($i = 2, \cdots, s$), and so $v_i \in T_2 \cap V_A(T_2) = K_2$ (Th. 7.2), which is a contradiction. Hence, $\{z_1, \cdots, z_t\}$ is still free over $V_A(T_2)$. Now, noting that $K_1 \subset V_A(T_1) \subset V_A(T_2)$, one will readily obtain $[T_2:V_{T_2}(Z)] = [K_2 \cdot Z:K_2] \leqslant [K_1 \cdot Z:K_1] = [T_1:V_{T_1}(Z)]$.