Lemma 12.9. <u>Let</u> A <u>be finite Galois over</u> B, <u>and</u> T <u>an intermediate ring of</u> A/B.

(a) <u>If</u> V <u>is a division ring then for every</u> v <u>in</u> $V_T(B)$ <u>there exists an element</u> t <u>such that</u> $T = V_T(Z)[t]$ <u>and</u> $B[t] \ni v$.

(b) <u>If</u> A <u>is a division ring then for every</u> v <u>in</u> $V_T(Z)$ <u>there exists an element</u> t <u>such that</u> $T = V_T(Z)[t]$ <u>and</u> $B[t] \ni v$.

<u>Proof</u>. (a) Recall that every intermediate ring of A/B is a simple ring (Prop. 7.3 (b)). In virtue of Cor. 11.8, it suffices to prove our assertion for the case $[B:Z] < \infty$ and $v \neq 0$. Now, let $\{x_1, \dots, x_p\}$ be a Z-basis of B. Since $V_T(Z) = B \otimes_Z V_T(B)$ by Prop. 4.8, $\{x_1, \dots, x_p\}$ is a $V_T(B)$-basis of $V_T(Z)$. By Cor. 7.11, T is inner Galois and finite over its center C'. If $\{z_1, \dots, z_q\}$ is a C'-basis of $Z\cdot C'$ taken from Z, then $\mathfrak{T} = \mathfrak{G}(T/V_T(Z))\cdot(V_T(Z))_R = \widetilde{Z\cdot C'}\cdot(V_T(Z))_R = \oplus_1^q \tilde{z}_i(V_T(Z))_R$. Since $V_T^2(Z) = Z\cdot C' \subset V_T(Z)$, T is $\mathfrak{T}$-isomorphic to $\mathfrak{T}$ (Cor. 9.5). If $t' \in T$ corresponds to $1 \in \mathfrak{T}$ under the above isomorphism then $\{t'\tilde{z}_1, \dots, t'\tilde{z}_q\}$ is a right $V_T(Z)$-basis of T, and so $1 = \sum_1^q (t'\tilde{z}_i)u_i'$ with $u_i' = \sum_1^p x_j v_{ji}' \in V_T(Z) = B \otimes_Z V_T(B)$ $(v_{ji}' \in V_T(B))$. Here, without loss of generality, we may assume $v_{11}' \neq 0$. If $t = t'v_{11}'v^{-1}$ then it is easy to see that $\{t\tilde{z}_1, \dots, t\tilde{z}_q\}$ is still a right $V_T(Z)$-basis of T (whence $T = V_T(Z)[t]$) and $1 = \sum_1^q t\tilde{z}_i\cdot u_i$ $(u_i \in V_T(Z))$ with $u_1 = x_1 v + x_2 v_2 + \dots + x_p v_p$ $(v_j \in V_T(B))$. As $[T:V_T(Z))] \geqslant [B[t]:V_{B[t]}(Z)]$ (Lemma 12.8), $\{t\tilde{z}_1, \dots, t\tilde{z}_q\}$ is a right $V_{B[t]}(Z)$-basis of $B[t]$, too. Hence, we see that every u_i is contained in $B[t]$. If σ is an arbitrary element of $\mathfrak{G}(B[t])$ then $u_1 = u_1\sigma = x_1\cdot v\sigma + x_2\cdot v_2\sigma + \dots + x_p\cdot v_p\sigma$, and so, recalling that $v\sigma$ and every $v_i\sigma$ are in V and $\{x_1, \dots, x_p\}$ is a V-basis of $B\cdot V$, it follows at once $v = v\sigma$, namely, $v \in B[t]$ (Th. 7.2).

(b) In the proof of (a), we may assume that $u_1' \neq 0$ $(\in V_T(Z))$. If this time we set $t = t'u_1'v^{-1}$ then $\{t\tilde{z}_1, \dots, t\tilde{z}_q\}$ is still a right $V_T(Z)$-basis of T and $1 = \sum_1^q (t\tilde{z}_i)u_i$ $(u_i \in V_T(Z))$ with $u_1 = v$. Hence, noting that $[T:V_T(Z)] \geqslant [B[t]:V_{B[t]}(Z)]$ (Lemma 12.8), we see that $\{t\tilde{z}_1, \dots, t\tilde{z}_q\}$ forms a right $V_{B[t]}(Z)$-basis of $B[t]$, which proves evidently $v = u_1 \in B[t]$.

Let S be a unital subring of $R \ni 1$. If $R = S[x_1, \dots, x_k]$ for some $x_1, \dots, x_k$ $(k > 0)$ and if $R = S[y_1, \dots, y_s]$ $(s > 0)$ yields always $k \leqslant s$, then (the uniquely determined) k will be denoted by $k(R/S)$. Needless to say, $k(R/S) = 1$ means that R is singly generated over S. In case A is finite Galois over B, we set $k_o = \max k(W/Z)$ $(\leqslant [V:Z] < \infty)$, where W ranges over all the intermediate rings of V/Z.

We are now at the prosition to prove the following:

Theorem 12.10. _Let_ A _be finite Galois over_ B.

(a) _If_ V _is a division ring then_ $k(T/B) \leqslant k_o$ _for every intermediate ring_ T _of_ A/B.

(b) _Let_ A _be a division ring_. _In order that every intermediate ring of_ A/B _be singly generated over_ B, _it is necessary and sufficient that_ $[B:Z] \geqslant k_o$.

Proof. (a) If $[B:Z] = \infty$, there is nothing to prove (Cor. 11.8). Assume now that $[B:Z] < \infty$. Then, $V_T(Z) = B \otimes_Z V_T(B)$ by Th. 4.8. If $V_T(B) = Z[v_1, \dots, v_s]$ $(s = k(V_T(B)/Z) \leqslant k_o)$, then there exists an element t such that $T = V_T(Z)[t]$ and $B[t] \ni v_1$ (Lemma 12.9 (a)), so that it follows $B[t, v_2, \dots, v_s] = B[t, v_1, v_2, \dots, v_s] = V_T(Z)[t] = T$, which proves our assertion $k(T/B) \leqslant k_o$.

(b) Again by Cor. 11.8, we may restrict our attention to the case that B possesses a finite Z-basis $\{x_1, \dots, x_p\}$. One may remark again $V_T(Z) = B \otimes_Z V_T(B)$ for any intermediate ring T of A/B. Assume first that $p \geqslant k_o$, and let $V_T(B) = Z[v_1, \dots, v_s]$ $(s \leqslant k_o)$. If $v = \sum_1^s x_i v_i$ $(\in V_T(Z))$ then for every σ in $\mathfrak{G}(A/B[v])$ we obtain $v = v\sigma = \sum_1^s x_i \cdot v_i\sigma$, whence it follows $v_i\sigma = v_i$. Hence, every v_i is contained in $B[v]$. Now, it is obvious that $T = B[t]$ with some t (Lemma 12.9 (b)). Next, we shall prove the converse. Let W be an intermediate ring of V/Z such that $k(W/Z) = k_o$. We have then $B \cdot W = B \otimes_Z W = B[t]$ with some $t = \sum_1^p x_i w_i$ $(w_i \in W)$. Since $B[w_1, \dots, w_p] = B[t]$, it follows at once $W = Z[w_1, \dots, w_p]$, and hence $p \geqslant k_o$.

Corollary 12.11. <u>Let a division ring</u> A <u>be Galois and finite over</u> B <u>with perfect</u> Z. <u>If</u> $B \neq Z$ <u>or</u> V <u>is commutative then every intermediate ring of</u> A/B <u>is singly generated over</u> B, <u>and conversely</u>.

<u>Proof</u>. Every intermediate ring W of V/Z is a separable division algebra of finite rank over Z, and so $k(W/Z) \leqslant 2$ (Th. 11.10). It follows therefore $k_o \leqslant 2$, and then by the validity of Th. 12.10 (b) all the intermediate rings of A/B are singly generated over B if and only if $[B:Z] \geqslant 2$ or $k_o = 1$.

Let A_1 and A_2 be non-commutative central division algebras of finite rank over the rational number field C such that $[A_1:C]$ and $[A_2:C]$ are relatively prime (cf. Köthe [1]). Then, the central division algebra $A = A_1 \otimes_C A_2$ (Cor. 4.4) is inner Galois and finite over the field $B = C[a]$ $(a \in A_1 \setminus C)$. As evidently $B \not\subset C$, A is singly generated over B by Th. 11.16 (a). However, every intermediate ring of A/B does not have to be so. In fact, $V = V_{A_1}(B) \otimes_C A_2$ is a non-commutative intermediate ring of A/B and $C_o = B$, which means $k(V/B) > 1$ (cf. Cor. 12.11).

Lemma 12.12. <u>Let</u> A <u>be finite Galois over</u> B, <u>and</u> T <u>in</u> $\mathfrak{R}$. <u>If</u> B <u>is not contained in the center</u> C' <u>of</u> T <u>then</u> $k(T/B) \leqslant \max\{0, k(Z\cdot C'/Z) - [B:Z]\} + 2$.

<u>Proof</u>. In case $[B:Z] = \infty$, our assertion is clear by Cor. 11.8. We may assume therefore $[B:Z] < \infty$. We have then $[T:C'] < \infty$ (Cor. 7.11), and so $T = C'[B, t]$ with some t (Th. 12.1). Now, let $\{x_1, \dots, x_p\}$ be a Z-basis of B, and $Z\cdot C' = Z[t_1, \dots, t_q]$ $(q = k(Z\cdot C'/Z))$. If $u = \sum_1^s x_i t_i$ $(s = \min\{p, q\})$ then $T^* = B[t, u, \{t_i; s < i \leqslant q\}]$ is a simple subring (Prop. 3.8 (a)). Since $B\cdot V = B \otimes_Z V$, if y is in $V_A(T^*) (\subset V)$ then $0 = yu - uy = \sum_1^s x_i(yt_i - t_iy)$ implies $yt_i = t_iy$ $(i = 1, \dots, s)$. It follows

therefore $V_A(T^*) = V_A(B[t, t_1, \dots , t_q]) = V_A(T)$, which means that T^* is a regular subring of A. For every σ in $\mathfrak{G}(A/T^*)$ (cf. Th. 7.2), there holds $0 = u - u\sigma = \sum_1^s x_i(t_i - t_i\sigma)$. Recalling here that V is $\mathfrak{G}$-invariant, it follows $t_i = t_i\sigma$, whence we see that $t_i \in T^*$. We have proved therefore $T = T^*\cdot C' = T^* = B[t, u, \{ t_i ; s < i \leq q\}]$, which implies our assertion.

Corollary 12.13. Let A be Galois and finite over B, and $k_1 = \max k(U'/Z)$ where U' ranges over all the commutative intermediate rings of V/Z. If $[B:Z] \geq k_1$ then $k(T/B) \leq 2$ for every $T \in \mathcal{R}$.

Proof. In case B is not contained in the center C' of T, our assertion is obvious by Lemma 12.12. On the other hand, if $B \subset C'$ then $V \supset T$ and $1 = [B:Z] \geq k_1$, namely, $k_1 = 1$. Since $T = C'[u, v]$ (Th. 11.10), it is easy to see that $k(T/B) \leq k(C'[u]/Z) + 1 = 2$.

We shall conclude this section with the following partial extension of Th. 12.10 (a).

Theorem 12.14. Let A be finite Galois over B, and T a regular intermediate ring of A/B. If $B \neq Z$ then $k(T/B) \leq k_o$.

Proof. If $k_o = 1$ then V is commutative, and hence $k(T/B) = 1$ (Th. 12.4). Thus, in what follows, we may assume that $k_o > 1$. Obviously, B is not contained in the center C' of T. If $k(Z\cdot C'/Z) - [B:Z] \leq 0$ then $k(T/B) \leq 2$ by Lemma 12.12. While, if $k(Z\cdot C'/Z) - [B:Z] > 0$ then $k(T/B) \leq k(Z\cdot C'/Z) - [B:Z] + 2 \leq k(Z\cdot C'/Z) \leq k_o$ again by Lemma 12.12.

Kishimoto-Nagahara-Tominaga [1]; Nagahara [4]; Nagahara-Tominaga [6], [7].

13. Extension with a Galois group of order p^e

In this section, we use the same conventions as in §11. Moreover, $\mathfrak{G}$ means an automorphism group of A, and p a prime number.

Lemma 13.1. *Let* A *be a* p *dimensional field extension of a field* B *not of characteristic* p. *If* $A = B[a] = B[a']$ *and* $a^p, a'^p \in B$ *then there exist an element* b *in* B *and an integer* ν *such that* $a' = ba^{\nu}$.

Proof. If ζ is a primitive p-th root of 1 then the polynomials $\lambda^p - a^p$ and $\lambda^p - a'^p$ are still irreducible as polynomials in $(B[\zeta])[\lambda]$. Hence $A[\zeta] = B[\zeta, a]$ is a p dimensional cyclic extension of $B[\zeta]$, and so there holds $\bigcup_0^{p-1} a^i B[\zeta]^{\cdot} = \bigcup_0^{p-1} a'^i B[\zeta]^{\cdot}$ (cf. Remark to Th. 10.10). There exist therefore an element $b \in B[\zeta]$ and an integer ν $(0 < \nu < p)$ such that $a' = a^{\nu} b$. We have then $b = a'a^{-\nu} \in B[\zeta] \cap A = B$.

Theorem 13.2. *Let* $\mathfrak{G}$ *be an F-group of order* p^e *with* $B = J(\mathfrak{G})$, *and* $p^f = (\mathfrak{G} : \mathfrak{G} \cap \tilde{V}) \cdot p^{\varepsilon}$, *where* p^{ε} *is the exponent of the group* $\mathfrak{G} \cap \tilde{V}$.

(a) *If* Z *contains no primitive* p-*th roots of* 1 *then* [A:B] *is a multiple of* p^f *and a divisor of* p^e.

(b) *If* A *is not of characteristic* p, *and* Z *contains no primitive* p-*th roots of* 1 *then* [A:B] *coincides with* p^e.

(c) *Let* A *be of characteristic* p. *If* V/C *is singly generated then* [A:B] *coincides with* p^f, *and conversely*.

Proof. As $\mathfrak{G}$ is a p-group and Z contains no primitive p-th roots of 1, V coincides with the field $C \cdot Z$ and contains no primitive p-th roots of 1 (Lemma 10.4). Now, we shall divide the proof into three steps.

(1) At first, by the induction with respect to e we shall prove that [A:B] divides p^e. If $e = 1$ then $\mathfrak{G}$ is either outer or inner. If $\mathfrak{G}$ is outer then $[A:B] = p$ by Th. 7.4. While, if $\mathfrak{G}$ is inner: $\mathfrak{G} = \{\tilde{1}, \tilde{v}, \ldots, \tilde{v}^{p-1}\}$ then $V = C \cdot Z = Z$ and $v^p = c \in C$. Since $\lambda^p - c$ is irreducible, $p = [C[v]:C] = [V:C] = [A:B]$ (Th. 7.7).

Now, assume $e > 1$. Then, as is well known, the center of $\mathfrak{G}$ contains a subgroup $\mathfrak{P}$ of order p. As $\mathfrak{P}$ is obviously a DF-group, $P = J(\mathfrak{P})$ is simple and $V_P(P)$ ($\subset V$) contains no primitive p-th roots of 1. Hence, $[A:P] = p$ by the case $e = 1$. Further, noting that $V_P(B)$ is a subfield of V, $P|\mathfrak{G}$ is a DF-group of P, and so $[P:B]$ divides the order of $P|\mathfrak{G}$ that is a divisor of p^{e-1}. Hence, we see eventually $[A:B]$ divides p^e.

(2) We shall prove (b) by the induction with respect to e. The case $e = 1$ has been shown in (1). Assume $e > 1$, choose a subgroup $\mathfrak{P}$ of order p contained in the center of $\mathfrak{G}$, and set $P = J(\mathfrak{P})$. Then, as was noted in (1), $\mathfrak{P}$ and $P|\mathfrak{G}$ are DF-groups of A and P respectively, and the center of P contains no primitive p-th roots of 1. It follows therefore $[A:B] = [A:P]\cdot[P:B] = p\cdot\#(P|\mathfrak{G})$ by the induction hypothesis. If $\mathfrak{P}$ is outer then $\mathfrak{G}(P) = \mathfrak{P}$ (Th. 7.4). Assume now that $\mathfrak{P}$ is inner: $\mathfrak{P} = \{\tilde{1}, \tilde{v}, \dots, \tilde{v}^{p-1}\}$, and that there exists an element $\tilde{u}$ in $\mathfrak{G}(P)\setminus\mathfrak{P}$ (cf. Th. 7.2). Since $p = [V_A(P):C] = [C[v]:C] = [C[u]:C]$ (Th. 7.7), the defining equation of u over C is of the form $f(\lambda) = \lambda^p + \dots + c_p$. If $u^{p^e} = c' \in C$ and ζ is a primitive p^e-th root of 1, then $-c_p = u^p\zeta^j$ with some j. Hence, as $V_A(P)$ contains no primitive p-th roots of 1, it follows $-c_pu^{-p} = \zeta^j = 1$, namely, $u^p = -c_p \in C$. Combining the above with $V_A(P) = C[v]$ and $v^p \in C$, we see that there exist $c \in C$ and ν such that $u = v^\nu c$ (Lemma 13.1), whence it follows a contradiction $\tilde{u} = \tilde{v}^\nu \in \mathfrak{P}$. We have seen thus $\mathfrak{G}(P) = \mathfrak{P}$ in either case. Accordingly, we obtain $[A:B] = p\cdot\#(P|\mathfrak{G}) = p\cdot(\mathfrak{G}:\mathfrak{P}) = p^e$.

(3) If A is of characteristic p, then the field $V = I(\mathfrak{G} \cap \tilde{V})$ is a finite dimensional purely inseparable extension of C and one will easily see that the exponent of V/C coincides with ε. Hence, p^ε divides $[V:C] = [A:H]$, and so $p^f = p^\varepsilon\cdot(\mathfrak{G} : \mathfrak{G} \cap \tilde{V})$ does $[A:H]\cdot(\mathfrak{G} : \mathfrak{G} \cap \tilde{V}) = [A:H]\cdot[H:B] = [A:B]$ (Ths. 7.7 and 7.4). This together with (1) and (2) proves (a). If p^ε coincides with $[V:C] = [A:H]$, or, if p^f coincides with $[A:B]$ then V/C is singly generated, and conversely (cf. van der Waerden [1]).

Let A be of characteristic p, and $\mathfrak{G}$ an F-group of order p^e with $B = J(\mathfrak{G})$. Then, $\mathfrak{G} \cap \tilde{V}$ is abelian (Lemma 10.4), and so we may set $\mathfrak{G} \cap \tilde{V} = \mathfrak{G}_1 \times \dots \times \mathfrak{G}_t$ with cyclic $\mathfrak{G}_i$. As $V_i = I(\mathfrak{G}_i)$ is evidently singly generated over C, $[V_i : C] =$ exponent of $\mathfrak{G}_i = \# \mathfrak{G}_i$ and $V = V_1 \dots V_t$ (Lemma 10.4). Accordingly, one will easily see the following:

Corollary 13.3. *Let* A *be of characteristic* p, $\mathfrak{G}$ *an F-group of* A *with* $B = J(\mathfrak{G})$ *and* $\# \mathfrak{G} = p^e$. *In order that* A/B *be* $\mathfrak{G}$*-regular it is necessary and sufficient that* $V_1 \dots V_t = V_1 \otimes_C V_2 \dots \otimes_C V_t$. *In particular, if* $\mathfrak{G} \cap \tilde{V}$ *is cyclic then* A/B *is* $\mathfrak{G}$*-regular.*

Now, let Φ be a field, and G a group of finite order g. Then, as is well known, the group ring $\Phi(G)$ is semi-simple if and only if the characteristic of Φ does not divide g (Maschke). If A is a central simple algebra over C, then the group ring $A(G) = C(G) \otimes_C A$, and then Lemma 4.1 and Maschke's theorem prove the same assertion for $A(G)$. However, in the present stage, we take an interest in the case that Φ is of characteristic p and $g = p^e$.

Lemma 13.4. *If* Φ *is a field, and* G *a group of finite order* $g > 1$, *then the following conditions are equivalent*: (1) $\Phi(G)$ *is completely primary, that is, the residue class ring of* $\Phi(G)$ *modulo its radical is a division ring, and* (2) Φ *is of characteristic* p *and* $g = p^e$.

Proof. The mapping $\lambda : \sum_{\sigma \in G} \sigma x_\sigma \longrightarrow \sum x_\sigma$ is a ring homomorphism of $\Phi(G)$ onto Φ with the kernel $\operatorname{Ker} \lambda = \sum (1 - \sigma)\Phi$.
(1) $\Longrightarrow$ (2): The radical $\mathfrak{n}$ of the completely primary ring $\Phi(G)$ coincides with the set of all non-units, and so $\mathfrak{n} = \operatorname{Ker} \lambda$. If Φ is of characteristic 0 then $\sum_{\sigma \in G} \sigma$ is a unit, for $(\sum \sigma)\lambda = g \cdot 1 \neq 0$. But this contradicts $(\sum \sigma)(1 - \tau) = 0$ ($\tau \neq 1$ in G). Hence, has to be of prime characteristic p. We set here $g = p^e \cdot g'$, where $(g', p) = 1$. If q is a prime factor of g' then G contains a q-Sylow group Q, and $\alpha = \sum_{\sigma \in Q} \sigma$ is a unit, because $\alpha\lambda$ is a

power of q. While, for any $\tau \neq 1$ in Q we have $\alpha(1 - \tau) = 0$. This contradiction proves $g' = 1$. (2)$\Longrightarrow$(1): By the induction with respect to e, we shall prove that $\mathfrak{n} = \operatorname{Ker} \lambda$ is nilpotent. In case $e = 1$, $(1 - \sigma)^p = 0$ yields at once $\mathfrak{n}^p = 0$. Assume next $e > 1$, and choose a subgroup P of order p contained in the center of G. Then, the mapping $\mu : \sum_{\sigma \in G} \sigma x_\sigma \longrightarrow \sum \bar{\sigma} x_\sigma$ is a ring homomorphism of $\Phi(G)$ onto $\Phi(\bar{G})$, where $\bar{G} = G/P$ and $\bar{\sigma}$ denotes the residue class of σ modulo P. To be easily verified, Ker μ is nothing but the ideal generated by $\{1 - \eta;\ \eta \in P\}$. Since every $1 - \eta$ ($\eta \in P$) is contained in the center of $\Phi(G)$, $(\operatorname{Ker} \mu)^p = 0$. Moreover, as $(\operatorname{Ker} \lambda)\mu$ is contained in the radical of $\Phi(\bar{G})$, there holds $((\operatorname{Ker} \lambda)\mu)^k = 0$ for some k. It follows therefore $(\operatorname{Ker} \lambda)^{kp} = 0$, and our implication is evident.

Corollary 13.5. _If_ A _is a simple ring_, G _a finite group, and_ T _an invariant subgroup of_ G _of order_ $t > 1$, _then the following conditions are equivalent_: (I') $\sum_{\sigma \in G} \sigma x_\sigma$ _is a unit of_ A(G) _whenever_ $\sum \bar{\sigma} x_\sigma$ _is a unit of_ $A(\bar{G})$, _where_ $\bar{G} = G/T$ _and_ $\bar{\sigma}$ _is the residue class of_ σ _modulo_ T, _and_ (II') A _is of characteristic_ p _and_ $t = p^e$.

Proof. The mapping $\phi : \sum_{\sigma \in G} \sigma x_\sigma \longrightarrow \sum \bar{\sigma} x_\sigma$ defines a ring homomorphism of A(G) onto $A(\bar{G})$, and Ker ϕ is the ideal generated by $\{1 - \eta;\ \eta \in T\}$: $\operatorname{Ker} \phi = \sum_{\substack{\sigma \in G \\ \eta \in T}} \sigma(1 - \eta)A$. (I')$\Longrightarrow$(II'):

If α is an arbitrary element of Ker ϕ then $1 - \alpha$ is a unit as an inverse image of 1 relative to ϕ, and so there exists some β in A(G) such that $(1 - \alpha)(1 - \beta) = 1$, or $\alpha + \beta - \alpha\beta = 0$. Accordingly, if α is an idempotent then $\alpha = 0$, which means that Ker ϕ contains no non-zero idempotents. Hence, Ker ϕ is nilpotent (cf. § 3), whence the ideal $\sum_{\eta \in T} (1 - \eta)C$ of C(T) is nilpotent. The last fact implies evidently that C(T) is a completely primary ring. It follows therefore (C and so) A is of characteristic p and $t = p^e$ (Lemma 13.4). (II')$\Longrightarrow$(I'): Since C(T) is completely primary (Lemma 13.4), $\sum_{\eta \in T}(1-\eta)C$ is nilpotent. Noting that T is an invariant subgroup of G, one will readily see that $\operatorname{Ker} \phi$ is nilpotent, and then our implication is obvious.

Theorem 13.6. *Let* A/B *be* $\mathfrak{G}$*-regular, and* $\mathfrak{T}$ *an invariant F-subgroup of* $\mathfrak{G}$ *with* $T = J(\mathfrak{T})$. *If* $\# \mathfrak{T} = t > 1$ *and* $\bar{\mathfrak{G}} = \mathfrak{G}/\mathfrak{T}$ *then the following conditions are equivalent*: (I) $a \in A$ *is an* $\mathfrak{G}$*-n.b.e. whenever* $T_{\mathfrak{T}}(a)$ *is an* $\bar{\mathfrak{G}}$*-n.b.e., and* (II) B *is of characteristic* p *and* $t = p^e$.

Proof. By Cor. 9.9, A contains an $\mathfrak{G}$-n.b.e. u. Since $[T:B] = \# \bar{\mathfrak{G}} = \#(T|\mathfrak{G})$ (Lemma 10.2), $T_{\mathfrak{T}}(u)$ is an $\bar{\mathfrak{G}}$-n.b.e. of T. As in the proof of Cor. 13.5, the mapping $\phi : \sum_{\sigma \in \mathfrak{G}} \sigma x_{\sigma R} \longrightarrow \sum \bar{\sigma} x_{\sigma R}$ is a ring homomorphism of $\mathfrak{G} B_R$ ($\simeq B(\mathfrak{G})$) onto $\bar{\mathfrak{G}} B_R$ ($\simeq B(\bar{\mathfrak{G}})$) and one will easily see that $T_{\mathfrak{T}}(u\alpha) = (T_{\mathfrak{T}}(u))(\alpha\phi)$ for every $\alpha \in \mathfrak{G} B_R$. As $\mathfrak{G} B_R$ satisfies the minimum condition for one-sided ideals, $u\alpha$ is again an $\mathfrak{G}$-n.b.e. if and only if α is contained in $(\mathfrak{G} B_R)^{\cdot}$. Similarly, $T_{\mathfrak{T}}(u\alpha)$ is again an $\bar{\mathfrak{G}}$-n.b.e. if and only if $\alpha\phi$ is in $(\bar{\mathfrak{G}} B_R)^{\cdot}$. Now, our equivalence is a direct consequence of Cor. 13.5.

Corollary 13.7. *If* A/B *is* $\mathfrak{G}$*-regular, and* $\# \mathfrak{G} = h > 1$, *then the following conditions are equivalent*: (I_o) $a \in A$ *is an* $\mathfrak{G}$*-n.b.e. whenever* $T_{\mathfrak{G}}(a)$ *is in* $B^{\cdot}$, *and* (II_o) B *is of characteristic* p *and* $h = p^e$.

As a direct consequence of Cor. 13.7, we obtain the next:

Corollary 13.8. *Let* A *be a division ring of characteristic* p. *If* A/B *is* $\mathfrak{G}$*-regular and* $\# \mathfrak{G} = p^e$ *then it is completely basic*.

If A/B is Galois and $A = B \otimes_Z C$ then A is called a *trivial extension* of B. If A/B is a trivial extension then it is outer Galois and every $\mathfrak{G}$-invariant simple intermediate ring of A/B is a trivial extension of B (Lemma 4.1). While, if A is outer Galois over B then it is trivial, provided $\mathfrak{r}[B:Z] < \infty$ (Cor. 4.9). Now, assume that A/B is $\mathfrak{G}$-regular, B is of characteristic p, and that

$\# \mathfrak{G} = p^e$. If c is an element of C with $T_{\mathfrak{G}}(c) \neq 0$ then $\{c\sigma \; ; \; \sigma \in \mathfrak{G}\}$ is a B-basis of A contained in C (Cor. 13.7), and so $A = B \cdot C = B \otimes_Z C$. We obtain thus the following:

Corollary 13.9. *Assume that* A/B *is* $\mathfrak{G}$*-regular*, B *is of characteristic* p, *and that* $\# \mathfrak{G} = p^e$. *If* A/B *is trivial then* C *contains an element* c *with* $T_{\mathfrak{G}}(c) \neq 0$, *and conversely*.

Faith [1], [2]; Kishimoto-Onodera-Tominaga [1]; Moriya [1]; Nagahara-Onodera-Tominaga [1]; Onodera-Tominaga [1], [2]; Tominaga [6].

14. A problem concerning an extension with a cyclic Galois group

The present section is devoted exclusively to proving the following theorem that is trivially true for the commutative case.

Theorem 14.1. *Let* A *be Galois and finite over* B, *and* $B = J(\sigma)$ *for some* σ *in* $\mathfrak{G}$. *If* C *is infinite or* $[A:C] < \infty$ *then for any intermediate ring* B' *of* A/B *there exists some* $\tau \in \mathfrak{G}$ *such that* $J(\tau) = B'$.

Throughout the present section, *we assume always that* A *is finite Galois over* B, $B = J(\sigma)$ *with some* $\sigma \in \mathfrak{G}$, *and that* B' *is an arbitrary intermediate ring of* A/B. If $\Phi = B \cap C$ then the order γ of $C|\sigma$ coincides with $[C:\Phi]$. We set further $V' = V_A(B')$ and $Z' = V_{B'}(B')$.

Lemma 14.2. *If* $[A:C] < \infty$ *then there exists an element* z *in* Z *such that* $\sigma^\gamma = \tilde{z}$, $Z = \Phi[z]$ *and* $V = C[z] = C\cdot Z$, *and then* $J(\sigma^\gamma) = H = B\cdot C$ *and* $[H:B] = [V:Z] = \gamma$.

Proof. By Th. 7.7, $\sigma^\gamma = \tilde{s}$ with some $s \in V$. Since $c' = s\sigma\cdot s^{-1}$ is in C by $\sigma\tilde{s} = \tilde{s}\sigma$ and there holds $N_{C/\Phi}(c') = \prod_0^{\gamma-1} c'\sigma^i = 1$, it is well known that there exists an element $c \in C$ such that $c'^{-1} = c^{-1}\cdot c\sigma$ (cf. Th. 10.6). Setting $z = sc$, we see that $\tilde{s} = \tilde{z}$ and z is contained in $B \cap V = Z$. Hence, $C[z]$ is a subfield of C_o, and so $V = I([\sigma]) = I([\sigma^\gamma]) = C[z] = C\cdot Z$ (Prop. 7.1). Noting that $B\cdot C$ is simple as an intermediate ring of H/B (Prop. 7.3), it follows then $J(\sigma^\gamma) = H = B\cdot C = B\cdot V = B \otimes_Z V$ (Th. 7.7), which implies $[H:B] = [V:Z]$. Finally, recalling that C is finite Galois over $\Phi = C \cap Z = C \cap \Phi[z]$, it is easy to see that $[V:\Phi[z]] = [C:\Phi] = [V:Z]$, and hence $Z = \Phi[z]$.

Corollary 14.3. V *is a field*.

Proof. Obviously, $V|\sigma$ is an automorphism of V and $J(V|\sigma) = Z$. Since $[V:C_o] < \infty$, we obtain $V = C_o\cdot Z = C_o$ by Lemma 14.2.

As a consequence of Cor. 14.3, we see that B' is simple (Prop. 7.3), and the order β of $V|\sigma$ coincides with $[V:Z]$ and divides the order α of $H|\sigma$ that coincides with $[H:B]$ (Th. 7.4). We set here $\alpha' =$

α/β and $V = C[v]$ with some v such that $\sigma^\alpha = \tilde{v}$ (Prop. 7.1). Then, noting that C is finite Galois over Φ, V/Φ is singly generated, and hence there exist only a finite number of intermediate fields of V/Φ. If $H' = B' \cap H$ then $H' = J(H|\sigma^\varepsilon)$ with a positive divisor ε of α (Th. 7.4), whence it follows $J(\sigma^\varepsilon) = H'$. Thus, we realize that to our end it suffices to prove our theorem for B' with $B' \cap H = B$, and so, in what follows, <u>we always assume that</u> $B' \cap H = B$. Since there holds then $\mathcal{G}(V_A^2(B')/B') \simeq \mathcal{G}(H/B)$ by the contraction map (Cor. 7.8), $\mathcal{G}(B')$ contains an automorphism $\sigma\tilde{u}$ (Ths. 7.2 and 7.7), and so $J(\sigma\tilde{u}) \supset B'$. We have seen thus the set $\mathcal{J}$ consisting of all the intermediate rings T of A/B' such that $T = J(\sigma\tilde{u})$ for some $u \in V$ is non-empty. In the rest of this section, we shall use the following additional conventions: For arbitrary $u \in V$, we set $u_{**} = N_{V/Z}(u) = \prod_0^{\beta-1} u\sigma^i = (u_{**})^{\alpha'}$. If $T = J(\sigma\tilde{u})$ is in $\mathcal{J}$ then $T \cap H = B$ and $\mathcal{G}(V_A^2(T)/T) \simeq \mathcal{G}(H/B)$ by the contraction map, and then $(\sigma\tilde{u})^\alpha = \widetilde{vu_*}$ yields $V_A(T) = C[vu_*]$ (Prop. 7.1). Further, we set $V' = \Phi[d]$ with some fixed d, $\{V_A(T);\ T \in \mathcal{J}\} = \{V_A(T_1), \ldots, V_A(T_b)\}$, $g(\lambda) = \prod_0^{\alpha-1} (\lambda - d\sigma^\nu) = \sum_0^\alpha g_i\lambda^i$ $(g_\alpha = 1)$ and $f(\lambda) = \prod_0^{\beta-1} (\lambda - d\sigma^\nu) = \sum_0^\beta f_i\lambda^i$. Here, $g(\lambda)$ and $f(\lambda)$ are polynomials in $Z[\lambda]$ and $g(\lambda) = (f(\lambda))^{\alpha'}$.

Lemma 14.4. $Z' = V_B(B')$, B'/B <u>is inner Galois</u>, V' <u>is</u> σ-<u>invariant</u> <u>and</u> $[V':Z'] = \beta$. <u>If</u> $[A:C] < \infty$ <u>then</u> $V' = Z' \cdot C$.

<u>Proof</u>. Choose an arbitrary $T = J(\sigma\tilde{u})$ from $\mathcal{J}$. If x is in T then $x = x(\sigma\tilde{u})^\alpha = x\tilde{v}\tilde{u}_*$, namely, $x\tilde{v} = x\widetilde{u_*^{-1}}$. Hence, it follows $V_T(u_*) = V_T(v) = T \cap H = B$, which proves that T/B is inner Galois. Since $Z' \subset V_T(B) \subset V_T(u_*) = B$, B'/B is also inner Galois by Prop. 7.16. Next, $V' = V_A(B'\sigma\tilde{u}) = V'\sigma$. Finally, if $V'|\sigma^i = 1$ then $V_A(T)|\sigma^i = 1$, and then we obtain especially $v\sigma^i \cdot u_* = (vu_*)\sigma^i = vu_*$, namely, $v\sigma^i = v$. It follows therefore $V\,|\sigma^i = V'[v]\,|\sigma^i = 1$, and so we readily obtain β = order of $(V'|\sigma) = [V':V_B(B')] = [V':Z']$. Now, we shall prove the latter assertion. By the convention $B' \cap H = B$, we obtain $Z' \cap C = \Phi$. Then noting that C is finite Galois over Φ, it is easy to see that $Z' \cdot C = Z' \otimes_\Phi C$. Since $[V':Z'] = \beta = \gamma = [C:\Phi]$ (Lemma 14.2), our

assertion is a consequence of $Z' \cdot C = Z' \otimes_{\Phi} C$.

Corollary 14.5. <u>If</u> $T = J(\sigma\tilde{u}, A)$ <u>is in</u> $\mathcal{J}$ <u>then</u> $Z' = V_B(T)[g_o, \dots, g_{\alpha-1}]$.

<u>Proof</u>. As $V'\sigma = V'$ (Lemma 14.4), it is obvious that Z' contains $V_B(T)[f_o, \dots, f_{\beta-1}]$. On the other hand, as $V' = V_B(T)[d]$ and $f(d) = 0$, we obtain $[V':V_B(T)[f_o, \dots, f_{\beta-1}]] \leq \beta = [V':Z']$ (Lemma 14.4). Combining those, it follows at once $Z' = V_B(T)[f_o, \dots, f_{\beta-1}]$. Now, we shall distinguish between two cases.

Case I. The characteristic of A does not divide α': Obviously $U' = V_B(T)[g_o, \dots, g_{\alpha-1}]$ is contained in Z'. Recalling that $g(\lambda) = (f(\lambda))^{\alpha'}$, we see that $g_{\alpha-1} = \alpha' f_{\beta-1}$ (whence $f_{\beta-1} \in U'$) and $g_{\alpha-\mu} = \alpha' f_{\beta-\mu} + P(f_{\beta-\mu+1}, \dots, f_{\beta-1})$ where P is a polynomial with integral coefficients. Then, we can see inductively $f_{\beta-\mu} \in U'$ $(1 \leq \mu \leq \beta)$, and hence $U' \supset V_B(T)[f_o, \dots, f_{\beta-1}] = Z'$.

Case II. The characteristic of A is p dividing α': Since $V_A(T) = V[vu_*]$, it follows $V = V_A(T)[u_*] = V_A(T)[(u_{**}^p)^{\alpha'/p}] = V_A(T)[u_{**}^p]$, which proves that $V/V_A(T)$ is separable. Combining this with the fact that $V_A(T)$ is Galois and finite over $V_B(T)$ (cf. Lemma 14.4), we see that $V/V_B(T)$ is separable. Accordingly, if $q = p^s$ divides exactly α' then there holds $V_B(T)[f_o^q, \dots, f_{\beta-1}^q] = V_B(T)[f_o, \dots, f_{\beta-1}] = Z'$. Since $g(\lambda) = (f(\lambda)^q)^{\alpha'/q} = (f_o^q + f_1^q\lambda^q + \dots + \lambda^{\beta q})^{\alpha'/q}$ and p is no longer a divisor of α'/q, the same argument as in Case I enables us to obtain $Z' = V_B(T)[f_o^q, \dots, f_{\beta-1}^q] = V_B(T)[g_o, \dots, g_{\beta-1}]$.

Lemma 14.6. <u>Let</u> Ω <u>be a subset of</u> Φ, $k_o, k_1, \dots, k_q$ <u>elements of</u> Z' <u>with</u> $Z' = V_B(T)[k_o, \dots, k_q]$ <u>for every</u> $T \in \mathcal{J}$, <u>and let</u> $k(\lambda) = \sum_o^q k_i\lambda^i$. If Ω <u>is infinite then</u> Ω <u>contains an infinite subset</u> Ω' <u>such that</u> $Z' = V_B(T)[k(\omega')]$ <u>for every</u> $T \in \mathcal{J}$ <u>and</u> $\omega' \in \Omega'$.

<u>Proof</u>. Since there exist only a finite number of intermediate

fields between Z' and $V_B(T_1)$, we can find an intermediate field W of $Z'/V_B(T_1)$ such that the set $\Omega_1 = \{\ \omega \in \Omega\ ;\ V_B(T_1)[k(\omega)] = W\}$ is infinite. Now, for different elements $\omega_1, \ldots, \omega_{q+1}$ in Ω_1 the simultaneous equations with Vandermonde determinant

$$\lambda_o + \lambda_1\omega_i + \ldots + \lambda_q\omega_i^q = k(\omega_i) \quad (i = 1, \ldots, q + 1)$$

possess a unique solution, which is necessarily contained in W. Hence $(k_o, \ldots, k_q)$ being the unique solution, it follows $Z' = V_B(T)[k_o, \ldots, k_q] \subset W$, namely, $Z' = W$. We have proved therefore that $Z' = V_B(t_1)[k(\omega)]$ for every ω in Ω_1. Repeating the same argument for Ω_1 and T_2, and so on, one will obtain Ω' eventually.

Corollary 14.7. _If_ C _is infinite and_ q _is an arbitrary positive integer, then there exist different_ $\omega_1, \ldots, \omega_q \in \Phi\backslash\{d\}$ _such that_ $Z' = V_B(T)[\prod_s^t g(\omega_i)]$ _for every_ $T \in \mathcal{J}$ _and_ $s \leq t\ (1 \leq s, t \leq q)$.

Proof. Since Φ is infinite (by $[C:\Phi] < \infty$) and $Z' = V_B(T)[g_o, \ldots, g_{\alpha-1}, 1]$ for every $T \in \mathcal{J}$ (Cor. 14.5), there exists an infinite subset Ω_o of $\Phi\backslash\{d\}$ such that $Z' = V_B(T)[g(\omega)]$ for every $T \in \mathcal{J}$ and every $\omega \in \Omega_o$ (Lemma 14.6), whence our assertion for $q = 1$ is evident. Now, assume that $q > 1$ and $\omega_1, \ldots, \omega_{q-1}$ $(\in \Phi\backslash\{d\})$ have been chosen as desired: $Z' = V_B(T)[\prod_s^t g(\omega_i)]$ for every $T \in \mathcal{J}$ and every $s \leq t\ (1 \leq s, t \leq q - 1)$. We set here $u_\nu = \prod_\nu^{q-1} g(\omega_i)\ (\nu = 1, \ldots, q - 1)$. Since $Z' = V_B(T)[u_\nu] = V_B(T)[u_\nu g_o, \ldots, u_\nu g_{\alpha-1}, u_\nu]$ and $u_\nu g(\lambda) = u_\nu g_o + \ldots + u_\nu\lambda^\alpha$, $\Phi\backslash\{d\}$ contains an infinite subset Ω_1 such that $Z' = V_B(T)[u_1 g(\omega)]$ for every $T \in \mathcal{J}$ and every $\omega \in \Omega_1$ (Lemma 14.6). Next, again by Lemma 14.6, there exists an infinite subset Ω_2 of Ω_1 such that $Z' = V_B(T)[u_2 g(\omega)]$ for every $T \in \mathcal{J}$ and $\omega \in \Omega_2$. Repeating the same procedures step by step, we obtain an infinite subset Ω_{q-1} of Ω_{q-2} such that $Z' = V_B(T)[u_{q-1}g(\omega)]$ for every $T \in \mathcal{J}$ and $\omega \in \Omega_{q-1}$. Finally, as in the case $q = 1$, we can find an element ω_q in Ω_{q-1}

such that $Z' = V_B(T)[g(\omega_q)]$ for every $T \in \mathcal{J}$. Now, the validity of $Z' = V_B(T)[\prod_s^t g(\omega_i)]$ $(T \in \mathcal{J}, 1 \leq s \leq t \leq q)$ will be evident.

We are now at the position to prove the principal theorem.

Proof of Th. 14.1. We shall distinguish between two cases:

Case I. C is infinite: By Cor. 14.7, we can find distinct elements $\omega_1, \dots, \omega_{b+1}$ in $\Phi\backslash\{d\}$ such that $Z' = V_B(T)[\prod_s^t g(\omega_i)]$ for every $T \in \mathcal{J}$ and $s \leq t$ $(1 \leq s, t \leq b+1)$. Choose an arbitrary (fixed) $T = J(\sigma\tilde{u})$ from $\mathcal{J}$, and set $w_\kappa = \prod_1^\kappa (\omega_i - d)$ $(\in V')$ for $\kappa = 1, \dots, b+1$. Then, every $B_\kappa = J(\sigma\widetilde{uw_\kappa})$ is contained in $\mathcal{J}$, and $V_A(B_\kappa) = C[v(uw_\kappa)_*] = C[vu_* \prod_1^\kappa g(\omega_i)]$ (Prop. 7.1). Hence, we obtain $V_A(B_e) = V_A(B_f)$ for some $e < f$ $(1 \leq e, f \leq b+1)$. Noting that $\omega_i \neq d$, one will readily see that $\prod_{e+1}^f g(\omega_i)$ is contained in $V_A(B_f) \cap Z = V_B(B_f)$, whence it follows $V_B(B_f) = V_B(B_f)[\prod_{e+1}^f g(\omega_i)] = Z'$. Accordingly, there holds $[V':Z'] = [V_A(B_f):V_B(B_f)] = [V_A(B_f):Z']$ (Lemma 14.4), which forces $V' = V_A(B_f)$. Hence, it follows $V_{B_f}(B') = V_{B_f}(B_f)$. As B_f/B is inner Galois by Lemma 14.4, Th. 7.7 yields then $B' = B_f \in \mathcal{J}$.

Case II. C is finite and $[A:C] < \infty$: Again, choose an arbitrary $T = J(\sigma\tilde{u})$ from $\mathcal{J}$. Then, $T \cap C = \Phi$ and $\alpha = \beta = \gamma$ (Lemma 14.2), and hence $(\sigma\tilde{u})^\gamma = \tilde{v}_1$ for $v_1 = vu_*$. Accordingly, in the same way as in the proof of Lemma 14.2, we can find an element $z \in V_T(T) \subset V_B(B') = Z'$ such that $\tilde{v}_1 = \tilde{z}$ and $V_T(T) = \Phi[z]$. Choose an element z' such that $Z' = \Phi[z']$. Then, $V' = Z' \cdot C = C[z']$ (Lemma 14.4), and we can find an element $w \in V'$ such that $z' = z \cdot N_{V'/Z'}(w) = zw_*$ (Cor. 10.8 and Lemma 14.4). Evidently, $B'' = J(\sigma\widetilde{uw})$ is contained in $\mathcal{J}$, and $(\sigma\widetilde{uw})^\alpha = z'$ yields $V_A(B'') = C[z'] = V'$. Thus, the same argument as in the last part of Case I applies to obtain $B' = B'' \in \mathcal{J}$.

Bortfeld [1]; Inatomi [2]; Masuda [1]; Nagahara-Tominaga [6].

15. Existence of cyclic extensions

It is the purpose of this section to give the condition for a simple ring to have a cyclic extension, and to determine the types of cyclic extensions. The material comes from Kishimoto [2]. At first, for the sake of the subsequent study, we shall glance over the ring of non-commutative polynomials. Let S be a ring with 1, ρ an automorphism of S, and ∂ a ρ-derivation in S (i.e. an endomorphism such that $(st)\partial = s\partial\cdot t\rho + s\cdot t\partial$ for every s, t in S). Then $S[\lambda;\rho,\partial]$ means the ring of all the non-commutative polynomials in the indeterminate λ with coefficients in S (written on the right side), where the multiplication is defined by the distributive laws and the rule $s\lambda = \lambda(s\rho) + s\partial$ $(s \in S)$. In particular, we set $S[\lambda;\partial] = S[\lambda;1,\partial]$, $S[\lambda;\rho] = S[\lambda;\rho,0]$ (and $S[\lambda] = S[\lambda;1,0]$). In case S is a division ring, it is well known that $S[\lambda;\rho,\partial]$ is a right (left) principal ideal domain.

Lemma 15.1. Let ∂ be in $D(S, S)$.

(a) If $g = \sum_o^m \lambda^i s_i$ is an arbitrary element of $S[\lambda;\partial]$, and z is an element of the center of S with $z\partial = z$, then $g(-\delta_z)^m = g(z_L - z_R)^m = m!zs_m$.

(b) If s is an arbitrary element of S then $(\lambda + s)^m = \sum_o^m \binom{m}{i} \lambda^{m-i}\Delta_i(s)$ (in $S[\lambda;\partial]$), where $\Delta_o(s) = 1$ and $\Delta_i(s) = (\Delta_{i-1}(s))\partial + (\Delta_{i-1}(s))s$ $(i = 1, 2, \ldots)$.

Proof. (a) $g(-\delta_z)^m = (zg - gz)(-\delta_z)^{m-1} = (\lambda^{m-1}mzs_m + \ldots)(-\delta_z)^{m-1} = m!zs_m$ by the induction. (b) is easily seen by the induction with respect to m.

Lemma 15.2. Let τ be an automorphism of S.

(a) Let s be an arbitrary element of S. Then, the mapping Φ : $\sum \lambda^i s_i \longrightarrow \sum (\lambda + s)^i s_i\tau$ defines a ring automorphism of $S[\lambda;\partial]$ if and only if $\tau^{-1}\partial\tau - \partial = \delta_s$. In particular, for any z in the center of S, Φ: $\sum \lambda^i s_i \longrightarrow \sum (\lambda + z)^i s_i$ defines an S-ring automorphism of $S[\lambda;\partial]$.

(b) *Let* s *be an arbitrary element of* $S^{\cdot}$. *The mapping* Ψ: $\sum \lambda^i s_i \longrightarrow \sum (\lambda s)^i s_i \tau$ *defines a ring automorphism of* $S[\lambda;\rho]$ *if and only if* $\tau^{-1}\rho^{-1}\tau\rho = s$. *In particular, for any unit* z *of the center of* S, $\Psi: \sum \lambda^i s_i \longrightarrow \sum (\lambda z)^i s_i$ *defines an* S-*ring automorphism of* $S[\lambda;\rho]$.

Proof. The proof is easy, and may be left to readers.

If ρ is of finite order m, we set $N_R(s;\rho) = s\cdot s\rho\cdot \ldots \cdot s\rho^{m-1}$ and $N_L(s;\rho) = s\rho^{m-1}\cdot \ldots \cdot s\rho\cdot s$ $(s \in S)$, which will be called the right respective left ρ-*norm* of s.

Now, let S be a simple ring. If I is an arbitrary non-zero ideal of $\mathfrak{R} = S[\lambda;\rho,\partial]$, there exists a uniquely determined monic polynomial f such that $I = f\mathfrak{R} = \mathfrak{R}f$. In fact, f is the monic polynomial in I of the lowest degree, and called the *monic generator* of I. (Note that S is a simple ring.) Now, let g be a monic polynomial in $\mathfrak{R}$. If g does not generate the ideal $\mathfrak{R}$ but every proper left divisor of g does $\mathfrak{R}$, g is defined to be *w-irreducible*. Needless to say, if g is contained in the center of $\mathfrak{R}$ and irreducible then it is w-irreducible, and if S is a field and $\mathfrak{R} = S[\lambda]$ then the notion of w-irreducibility coincides with that of irreducibility. The next will be easily seen.

Lemma 15.3. *Let* S *be a simple ring. A non-zero ideal of* $S[\lambda;\rho,\partial]$ *is maximal if and only if its monic generator is w-irreducible.*

If A/B is $\mathfrak{G}$-regular and $\mathfrak{G}$ is cyclic, A is called a *cyclic extension* of B w.r.t. $\mathfrak{G}$. Finally, let A/B be a cyclic extension w.r.t. $\mathfrak{G}$, and an intermediate ring A' of A/B a cyclic extension of B w.r.t. $\mathfrak{G}'$. If $\mathfrak{G}' = A'|\mathfrak{G}$, A'/B is said to be *regularly embedded* in the cyclic extension A/B.

15a. Throughout the present subsection, we assume that B *is a simple ring of characteristic* p. One of the principal theorems is the following:

Theorem 15.4. (a) *In order that* B *have a* p *dimensional cyclic extension, it is necessary and sufficient that there exist* $\partial \in D(B,B)$

and $b \in B$ *such that* (1) $\partial^{\mathfrak{p}} = \delta_b$, $b\partial = 0$, *and* (2) $\lambda^{\mathfrak{p}} - b$ *is w-irreducible in* $\mathfrak{L} = B[\lambda;\partial]$. *More precisely, if there exist* ∂, b *satisfying* (1), (2) *then* $M = (\lambda^{\mathfrak{p}} - b)\mathfrak{L}$ *is a maximal ideal*, $A^* = B[y] = \mathfrak{L}/M$ *is a* p *dimensional cyclic extension of* B *with a generating automorphism* σ^* *defined by* $y\sigma^* = y + 1$, *and* $\partial = B|\delta_y$, *where* y *is the residue class of* λ *modulo* M. *Conversely, if* A *is a* p *dimensional cyclic extension of* B *w.r.t.* $\mathfrak{G} = [\sigma]$, *then we can find such* ∂, b *satisfying* (1), (2) *that there holds a* B-*ring isomorphism* $\phi^* : A^* \simeq A$ *with* $\phi^*\sigma = \sigma^*\phi^*$.

(b) *In order that* B *has a* p *dimensional outer cyclic extension, it is necessary and sufficient that there exist* ∂ *and* b *satisfying* (1), (2) *and* (3) $Z|\partial = 0$.

(c) *In order that* B *have a* p *dimensional inner cyclic extension it is necessary and sufficient that there exist* ∂ *and* b *satisfying* (1) *and* (4) $z\partial = z$ *for some non-zero* z *in* Z.

Proof. (a) and (b). To be easily verified, (1) is equivalent with $\lambda^{\mathfrak{p}} - b \in V_{\mathfrak{L}}(\mathfrak{L})$, and so (2) implies the maximality of M (Lemma 15.3). Hence, $A^* = \sum_0^{p-1} y^iB$ is a simple ring and $\{1, y, \ldots, y^{p-1}\}$ forms a free B-basis of A^*. Noting that $\lambda^{\mathfrak{p}} - b$ is left invariant by the ring automorphism $\Phi : \sum \lambda^i b_i \longrightarrow \sum (\lambda + 1)^i b_i$ (Lemma 15.2 (a)), we see that Φ induces in A^* a B-ring automorphism σ^* of order p such that $y\sigma^* = y + 1$. If $\sum_0^{p-1} y^i b_i$ is left invariant by σ^* then $\sum_0^{p-1} (y + 1)^i b_i = \sum_0^{p-1} y^i b_i$ yields $\binom{p-1}{p-2} b_{p-1} + b_{p-2} = b_{p-2}$ (Lemma 15.1 (b)), and hence $b_{p-1} = 0$. Repeating the same procedure, we readily obtain $b_{p-1} = \ldots = b_1 = 0$, namely, $J(\sigma^*) = B$. If σ^* is inner: $\sigma^* = \tilde{z}$, then z is contained in $V_{A^*}(B) \cap B = Z$ and $z^p \in C^* = V_{A^*}(A^*)$, whence we see that $C^*[z]$ is a subfield of Z, namely, $[\sigma^*]$ is an F-group. Moreover, one may remark that $y\tilde{z} = y + 1$ implies $z\partial = z \neq 0$, and so $Z|\partial \neq 0$. While, if σ^* is outer then $[\sigma^*]$ is obviously an F-group and $Z|\partial = B \cap C^*|\delta_y = 0$. Conversely, assume that A/B be a p dimensional cyclic extension w.r.t. $\mathfrak{G} = [\sigma]$. Then, in virtue of Th. 10.5 and its proof, there exists an element $x \in A$ such that $x\sigma = x + 1$, and then $b = x^p \in B$, $A = B[x] = \sum_0^{p-1} x^i B$, and $\partial = B|\delta_x$ is a derivation in B with $\partial^p = \delta_b$. Obviously, $\lambda - b$ is contained in the center of $\mathfrak{G} = B[\lambda;\partial]$. Since $\phi : \sum \lambda^i b_i \longrightarrow \sum x^i b_i$ is a B-ring homomorphism of $\mathfrak{G}$ onto A whose kernel contains M and $[\mathfrak{G}/M:B] = p$, $\phi^* : \sum_0^{p-1} y^i b_i \longrightarrow \sum_0^{p-1} x^i b_i$ is a B-ring isomorphism of A^* onto A such that $\phi^*\sigma = \sigma^*\phi^*$. Hence, M is maximal, and so $\lambda^p - b$ is w-irreducible, completing the proof of (a). Now, (b) is obvious by the above proof.

(c) By the above proof, it suffices to prove that $\lambda^p - b$ is w-irreducible. If g is a proper monic left divisor of the central monic polynomial $\lambda^p - b$, then $\deg g = m < p$ and $g(-\delta_z)^m = m!z \neq 0$ (Lemma 15.1 (a)), which proves that g generates $\mathfrak{G}$, namely, $\lambda^p - b$ is w-irreducible.

Corollary 15.5. *Assume that* B *is a division ring. In order that* B *have a* p *dimensional cyclic division ring extension, it is necessary and sufficient that there exist* ∂ *and* b *satisfying* (1) *in Th.* 15.4 *and* (2') $\lambda^p - b$ *is irreducible in* $B[\lambda;\partial]$. *The precise statement corresponding to that in Th.* 15.4 *is valid*.

Proof. Since (1) and (2') imply that M is a maximal one-sided ideal, A^* is a division ring. The rest of the proof will be obvious.

Corollary 15.6. *The following conditions are equivalent*: (1) B *has a* p *dimensional trivial cyclic extension*, (2) *there exists an element* $b \in Z$ *such that* $\lambda^p - b$ *is irreducible in* $Z[\lambda]$, *and* (3) *there exist an inner derivation* ∂ *and* b *satisfying* (1), (2) *in Th*. 15.4.

Proof. (1)$\Longrightarrow$(2)$\Longrightarrow$(3): If A is a p dimensional trivial extension of B w.r.t. $[\sigma]$, then C is a p dimensional cyclic extension field of Z. Hence, there exists an element $b \in Z$ such that $\lambda^p - b$ is irreducible in $Z[\lambda]$. The latter is trivial. (3) $\Longrightarrow$(1): If $\partial = \delta_{b'}$, then $c = y - b'$ is contained in the center C^* of A^*, and $c\sigma^* = c + 1$. Hence, $A^* = \sum_0^{p-1} c^i B = B \otimes_Z C^*$.

Corollary 15.7. *Let* A/B *be* $\mathfrak{G}$*-regular. If* Z *is a perfect field of prime characteristic* p *and* $\mathfrak{G}$ *is of order* p^e, *then* A/B *is outer Galois. If moreover* $[B:Z] < \infty$ *then* A/B *is trivial.*

Proof. Since any derivation of the perfect field Z into B is zero, the case $e = 1$ is obvious by Th. 15.4 (c). Now, we shall proceed by the induction with respect to e. Assume $e > 1$. If $\mathfrak{G}$ contains an inner automorphism different from 1, then $\mathfrak{G}_o = \mathfrak{G} \cap \tilde{V}$ is an invariant DF-subgroup of $\mathfrak{G}$ (Lemma 10.4), and $B_o = J(\mathfrak{G}_o)$ is $(B_o|\mathfrak{G})$-regular over B (Lemma 10.2). Noting that B_o/B is outer Galois by the induction hypothesis, we see that the center of B_o is still perfect. As is well known, $\mathfrak{G}_o$ contains an invariant subgroup $\mathfrak{P}$ of order p. Then, $J(\mathfrak{P})/B_o$ is $(J(\mathfrak{P})|\mathfrak{G}_o)$-regular and the center of $J(\mathfrak{P})$ is perfect. Hence, by the case $e = 1$, $A/J(\mathfrak{P})$ is outer Galois, which is a contradiction. The second assertion is now contained in Cor. 4.9.

If B is a field and has a p dimensional cyclic extension field then, as is well known, B has a p^e dimensional cyclic extension field for every positive integer e. However, the same will be no longer valid for simple rings. Concerning the regular embedding of a p^e dimensional cyclic extension, we can prove the following:

Theorem 15.8. *Let* A'/B *be a cyclic extension w.r.t.* $\mathfrak{G}' = [\sigma']$ *of order* p^e. *In order that* A'/B *be regularly embedded in some* p^{e+1} *dimensional cyclic extension of* B, *it is necessary and sufficient that there exist* $\partial \in D(A', A')$ *and* $a', a'' \in A'$ *such that* (1) $\partial^{p} = \delta_{a'}$, $a'\partial = 0$, (2) $\lambda - a'$ *is w-irreducible in* $A'[\lambda;\partial]$, (3) $\sigma'^{-1}\partial\sigma' - \partial = \delta_{a''}$, (4) $T_{\mathfrak{G}'}(a'') \neq 0$ *and* (5) $\Delta_p(a'') - a'' = a'(\sigma' - 1)$.

Proof. By Lemma 15.2 (a), (3) means that $\Phi : \sum \lambda^i a_i' \longrightarrow \sum (\lambda + a'')^i a_i'\sigma'$ defines in $\mathfrak{A}' = A'[\lambda;\partial]$ an automorphism, whose order is p^{e+1} by (4). Next, (1) and (2) show that $M = (\lambda^p - a')\mathfrak{A}'$ is a maximal ideal and $A^* = \mathfrak{A}'/M$ is a p dimensional cyclic extension of A' (Th. 15.4). Since a brief computation with (5) and Lemma 15.1 (b) enables us to see that $\lambda^p - a'$ is left invariant by Φ,

Φ induces in A^* a B-ring automorphism σ^* of order p^{e+1} such that $y\sigma^* = y + a''$ and $A'|\sigma^* = \sigma'$, where y is the residue class of λ modulo M. If $\sum_0^{p-1} y^i a_i'$ is left invariant by σ^{*p^e} then $\sum_0^{p-1} y^i a_i' = \sum_0^{p-1} (y + T_{\mathfrak{G}'}(a''))^i a_i' = \sum_i \sum_{k=0}^{i} \binom{i}{k} y^{i-k} \Delta_k(T_{\mathfrak{G}'}(a''))a_i'$ (Lemma 15.1 (b)), whence it follows $a'_{p-2} = \binom{p-1}{p-2} \Delta_1(T_{\mathfrak{G}'}(a''))a'_{p-1} + a'_{p-2}$, namely, $T_{\mathfrak{G}'}(a'')\cdot a'_{p-1} = 0$. Since $bT_{\mathfrak{G}'}(a'') - T_{\mathfrak{G}'}(a'')b = T_{\mathfrak{G}'}(ba'' - a''b)$ $= T_{\mathfrak{G}'}(b(\sigma'^{-1}\partial\sigma' - \partial)) = T_{\mathfrak{G}'}(b\partial\sigma' - b\partial) = 0$ for every $b \in B$, $T_{\mathfrak{G}'}(a'')$ is a non-zero element of Z, and so we obtain $a'_{p-1} = 0$. Repeating the same argument, we readily obtain $a'_{p-1} = \dots = a'_1 = 0$, which proves evidently $J(\sigma^{*p^e}) = A'$. Hence, A/A' is cyclic w.r.t. $[\sigma^{*p^e}]$ and $J(\sigma^*) = J(\sigma') = B$. If A^*/A' is outer, the unique minimal subgroup $[\sigma^{*p^e}]$ of $\mathfrak{G}^* = [\sigma^*]$ is outer, and hence so is $\mathfrak{G}^*$ itself. On the other hand, if A^*/A' is inner then A' contains the center C^* of A^* and there exists a divisor p^g of p^e such that $\sigma^{*p^g} = \tilde{v} \in \tilde{V}^*$ $(V^* = V_{A^*}(B))$ and $\sigma^{*i} \notin \tilde{V}^*$ for every positive $i < p^g$. Obviously, v is contained in $J(\tilde{v}^{p^{e-g}}) \cap V^* = J(\sigma^{*p^e}) \cap V^* = V_{A'}(B)$. Since $V_{A'}(B)$ is a field (Lemma 10.4), $C^*[v]$ is its subfield. Hence, in either case, $\mathfrak{G}^*$ is an F-group. Conversely, assume that A'/B is regularly embedded in a cyclic extension A/B w.r.t. $\mathfrak{G} = [\sigma]$ of order p^{e+1}. Here, we may assume $\sigma' = A'|\sigma$. Since V is a field (Lemma 10.4) and $[A:A'] = p$, A/A' is cyclic w.r.t. $\mathfrak{G}(A') = [\sigma^{p^e}]$ (Lemma 10.2). Then, there exists an element x A such that $x\sigma^{p^e} - x = 1$ (Th. 10.1). Evidently, $a'' = x\sigma - x$ is contained in A' and $T_{\mathfrak{G}'}(a'') = 1$. Moreover, one will easily see that δ_x induces a derivation ∂ in A'. If we set $a' = x^{\mathfrak{F}}$ then, patterning after the proof of Th. 15.4, one will easily complete the proof.

15b. Throughout the present subsection, we assume that Z <u>contains a primitive</u> m-<u>th root</u> ζ <u>of</u> 1, <u>and a cyclic extension</u> A <u>of</u> B <u>will mean such one that the center</u> C <u>of</u> A <u>contains</u> ζ . At first, we shall deal with an m dimensional cyclic extension of B.

Lemma 15.9. *Let* ρ *be an automorphism of* B. *If there exists an element* $z_o \in Z^{\cdot}$ *such that* $z_o\rho = z_o\zeta$ *then any polynomial in* $B[\lambda;\rho]$ *of degree at most* $m - 1$ *with the non-zero constant term generates* $B[\lambda;\rho]$.

Proof. Let $f = \lambda^k b_k + \ldots + b_o$ $(0 \leq k < m,\ b_o \neq 0)$ be in $B[\lambda;\rho]$. Since the constant term of $z_of - fz_o\zeta^k$ is $b_oz_o(1 - \zeta^k) \neq 0$ and $\deg\,(z_of - fz_o\zeta^k) < k$, an easy induction will complete the proof.

Corresponding to Th. 15.4, we shall state the following:

Theorem 15.10. (a) *In order that* B *have an* m *dimensional cyclic extension, it is necessary and sufficient that there exist an automorphism* ρ *of* B *and* $b_o \in B^{\cdot}$ *such that* (1) $\rho^m = \tilde{b}_o^{-1}$, $b_o\rho = b_o$, $\zeta\rho = \zeta$, *and* (2) $\lambda^k - b_o$ *is w-irreducible in* $\mathcal{L}_k = B[\lambda;\rho^{k'}]$, *where* k *ranges over all the positive divisors of* m *and* $k' = m/k$. *More precisely, if there exist* ρ , b_o *satisfying* (1), (2) *then* $M = (\lambda^m - b_o)\mathcal{L}$ *is a maximal ideal of* $\mathcal{L} = B[\lambda;\rho]$ *and* $A^* = B[y] = \mathcal{L}/M$ *is a cyclic extension of* B *with a generating automorphism* σ^* *of order* m *defined by* $y\sigma^* = y\zeta$, *where* y *is the residue class of* λ *modulo* M. *Conversely, if* A/B *is an* m *dimensional cyclic extension w.r.t.* $\mathfrak{G} = [\sigma]$, *then we can find such* ρ , b_o *satisfying* (1), (2) *that there holds a* B-*ring isomorphism* $\phi^* : A^* \simeq A$ *with* $\phi^*\sigma = \sigma^*\phi^*$.

(b) *In order that* B *have an* m *dimensional outer cyclic extension, it is necessary and sufficient that there exist* ρ *and* b_o *satisfying* (1), (2) *and* (3) *if* $\rho^i = \tilde{b}$ *then* $b\rho = b$.

(c) *In order that* B *have an* m *dimensional inner cyclic extension, it is necessary and sufficient that there exist* ρ *and* b_o *satisfying* (1) *and* (4) $z_o\rho = z_o\zeta$ *for some* $z_o \in Z^{\cdot}$.

Proof. (a) and (b). Let k be an arbitrary positive divisor of m, and $k' = m/k$. To be easily seen, $\rho^m = \tilde{b}_o^{-1}$ and $b_o\rho = b_o$ imply that $\lambda^k b_o^{-1} - 1$ is contained in the center of $\mathcal{L}_k = B[\lambda;\rho^{k'}]$, and conversely. Hence, by (2), $M_k = (\lambda^k b_o^{-1} - 1)\mathcal{L}_k = (\lambda^k - b_o)\mathcal{L}_k$ is maximal (Lemma 15.3), and so $A_k^* = B[y_k] = \mathcal{L}_k/M_k$ is a simple ring and

$\{1, y_k, \ldots, y_k^{k-1}\}$ forms a B-basis of A^*_k, where y_k is the residue class of λ modulo M_k (and is a unit). Since $\lambda^k - b_o \in \mathfrak{G}_k$ is left invariant by the automorphism $\Psi_k : \sum \lambda^i b'_i \longrightarrow \sum (\lambda\zeta^{k'})^i b'_i$ (Lemma 15.2 (b)), Ψ_k induces in A^*_k a B-ring automorphism σ^*_k of order k such that $y_k\sigma^*_k = y_k\zeta^{k'}$ and $J(\sigma^*_k) = B$. Now, let k be especially the least positive integer such that σ_m^{*k} is inner: $\sigma_m^{*k} = \tilde{v}$. If $\sigma^* = \sigma^*_m$, $y = y_m$ and $A^* = A^*_m$, then $T^* = J(\sigma^{*k}) = \sum_o^{k-1} y^{k'i}B$. Noting that A^*_k is a simple ring, we see that $\phi^*_k : \sum_o^{k-1} y_k^i b'_i \longrightarrow \sum_o^{k-1} y^{k'i} b'_i$ defines a B-ring isomorphism of A^*_k onto T^*. Since v is contained in $J(\tilde{v}) \cap V_{A^*}(T^*) = V_{T^*}(T^*)$ and $v^{k'} \in C^* = V_{A^*}(A^*)$, $C^*[v]$ is a subfield of the center of the simple ring T^*, which proves that $[\sigma^*]$ is an F-group. Needless to say, $\zeta y = y(\zeta\rho) = v\zeta$, namely, ζ is contained in C^*. Now, let $a = \sum_o^{m-1} y^i d_i$ $(d_i \in B)$ be an arbitrary non-zero element of $V^* = V_{A^*}(B)$. Since $y^iB = By^i$, every $y^i d_i$ is contained in V^*. Hence, if d_i is non-zero then $(y^i d_i)B = B(y^i d_i)B = y^iBd_iB = y^iB$, whence we see that d_i is a unit and $\rho^i = \tilde{d}_i$. Accordingly, if (3) is satisfied then $d_i\rho = d_i$, which proves evidently $V^* = C^*$. Conversely, assume that A/B is an m dimensional cyclic extension w.r.t. $[\sigma]$. Then, there exists $x \in A^\cdot$ such that $x\sigma = x\zeta$ and $A = \oplus_o^{m-1} x^iB$ (Th. 10.6 and Cor. 10.9). If we set $\rho = B|x^{-1}$ and $b_o = x^m$, one will easily see that ρ is an automorphism of B, b_o is in B, and (1) is satisfied (cf. Th. 10.10). Moreover, if k is an arbitrary positive divisor of m, then $\lambda^k b_o^{-1} - 1$ is contained in the center of $\mathfrak{G}_k$ and A^*_k is isomorphic to the simple ring $J(\sigma^k) = \oplus_o^{k-1} x^{k'i}B$ (Cor. 14.3 and Prop. 7.3 (b)), which proves (2). Finally, assume that A/B is outer Galois and $\rho^i = \tilde{b}$. By the validity of (1), we may assume $0 \leq i < m$. Since $\rho^i = B|\tilde{x}^{-i}$, it follows $x^i b \in V = C$, and so $x^{i+1}\cdot b\rho = x^i bx = x^{i+1}b$, namely, $b\rho = b$.

(c) Under the above notations, the central monic polynomial $\lambda^m - b_o$ is w-irreducible by Lemma 15.9. Since $z_o y z_o^{-1} = y\cdot z_o\rho\cdot z_o^{-1} =$

$y\zeta$, we obtain $\sigma^* = \tilde{z}_o$. Accordingly, $V = J(V|\tilde{z}_o)$ coincides with the field Z. Hence, $[\sigma^*] = [\tilde{z}_o]$ is an F-group. Conversely, assume that A/B is an m dimensional inner cyclic extension w.r.t. $\mathfrak{G} = [\tilde{z}_o]$. Noting that $V = Z$ by Cor. 14.3, z_o is in Z and $z_o\rho = x^{-1}z_o x = x^{-1}\cdot x\tilde{z}_o\cdot z_o = z_o\zeta$.

The next will be almost evident (cf. Cor. 15.5).

Corollary 15.11. Let B be a division ring. In order that B have an m dimensional cyclic division ring extension, it is necessary and sufficient that there exist ρ, b_o satisfying (1) in Th. 15.10 and (2') $\lambda^m - b_o$ is irreducible in $B[\lambda;\rho]$. The precise statement corresponding to that in Th. 15.10 is valid.

Corollary 15.12. The following conditions are equivalent: (1) B has an m dimensional trivial cyclic extension, (2) there exists an element $b_o \in Z$ such that $b_o^{1/m} \notin Z$ and (3) there exist an inner automorphism ρ of B and $b_o \in B^\cdot$ satisfying (1), (2) in Th. 15.10.

Proof. The implications (1)$\Longrightarrow$(2)$\Longrightarrow$(3) are obvious. (Note that ζ is in Z.) We shall prove (3)$\Longrightarrow$(1). Under the notations in the proof of Th. 15.10, if $\rho = \tilde{b}$ then $c = yb$ is contained in C^* and $c\sigma^* = c\zeta$. Hence, $A^* = B[c] = B \otimes_Z C^*$ (Cor. 10.9).

Corresponding to Th. 15.8, the regular embedding probelem for the present case is solved in the following way:

Theorem 15.13. Let A'/B be an m' dimensional cyclic extension w.r.t. $\mathfrak{G}'$. In order that A'/B be regularly embedded in some $m'm$ dimensional cyclic extension, it is necessary and sufficient that there exist a generator σ' of $\mathfrak{G}'$, an automorphism ρ of A', and units a', a'' of A' such that (1) $\rho^{m'} = a'^{-1}$, $a'\rho = a'$, $\zeta\rho = \zeta$, (2) $\lambda^m - a'$ is w-irreducible in $A'[\lambda;\rho]$, (3) $\sigma'^{-1}\rho^{-1}\sigma'\rho = \tilde{a}''$, (4) $N_R(a'';\sigma') = \zeta$, (5) $a'\sigma' = a'\cdot a''\rho^{m-1}\cdot \ldots \cdot a''\rho\cdot a''$ and (6) if $(a_o', a_1', \ldots, a_{m-1}')$ is a non-zero $1 \times m$ matrix with components in A' and $b\rho^i\cdot a_i' = a_i'b$ for every $b \in B$ $(i = 0, 1, \ldots, m-1)$ then the simultaneous equations $\sum_o^k a_{k-i}'\rho^i\cdot u_i + \sum_{k+1}^{m-1} a'\cdot a_{m+k-i}'\rho^i\cdot u_i = \delta_{ok}$ $(k = 0, 1, \ldots, m-1)$ have a solution in A'.

Proof. By Lemma 15.2 (b), (3) means that $\Psi : \sum \lambda^i a_i' \longrightarrow$

$\sum (\lambda a'')^i a_i' \sigma'$ defines in $\mathfrak{A}' = A'[\lambda;\rho]$ an automorphism, whose order is $m'm$ by (4). Next, (1) and (2) show that $M = (\lambda^m - a')\mathfrak{A}'$ is a maximal ideal of $\mathfrak{A}'$, $A^* = \mathfrak{A}'/M$ is a simple ring with $\{1, y, \ldots, y^{m-1}\}$ as a B-basis, where y is the residue class of λ modulo M. Since (5) implies that $\lambda^m - a'$ is left invariant by Ψ, Ψ induces in A^* a B-ring automorphism σ^* of order $m'm$ such that $y\sigma^* = ya''$ and $A'|\sigma^* = \sigma'$. To be easily seen, $J(\sigma^{*m'}) = A'$, and so $J(\sigma^*) = B$. Finally, if $v = \sum_0^{m-1} y^i a_i'$ is a non-zero element of $V_{A^*}(B)$ then $b\rho^i \cdot a_i' = a_i' b$ and (6) secures the existence of the inverse of v, which means that $V_{A^*}(B)$ is a division ring. Conversely, assume that A'/B is regularly embedded in the $m'm$ dimensional cyclic extension A/B w.r.t. $\mathfrak{G} = [\sigma]$, and set $\sigma' = A'|\sigma$. Since V is a field (Cor. 14.3) and $[A:A'] = m$, A/A' is cyclic w.r.t. $\mathfrak{G}(A') = [\sigma^{m'}]$ (Lemma 10.2). Then, there exists an element $x \in A^{\cdot}$ such that $x\sigma^{m'} = x\zeta$ (Th. 10.6). Evidently, $a'' = x^{-1} \cdot x\sigma$ is contained in A' and $N_R(a'';\sigma') = x^{-1} \cdot x\sigma^{m'} = \zeta$. Moreover, $\widetilde{x}^{-1}$ induces an automorphism ρ of A'. If we set $a' = x^m$ then, patterning after the proof of Th. 15.10, we can see the validity of the conditions (1), (2), (3), (5) and (6).

The condition (6) in Th. 15.13 was needed only to see that the centralizer of B in the extension considered is simple. Accordingly, combining Th. 15.13 with Cor. 15.11, we readily obtain the following:

Corollary 15.14. _Let_ A'/B _be an_ m' _dimensional cyclic division ring extension w.r.t._ $\mathfrak{G}'$. _In order that_ A'/B _be regularly embedded in some_ $m'm$ _dimensional cyclic division ring extension, it is necessary and sufficient that there exist a generator_ σ' _of_ $\mathfrak{G}'$, _an automorphism_ ρ _of_ A' _and non-zero elements_ a', a'' _of_ A' _such that_ (1) $\rho^{m'} = \widetilde{a'}^{-1}$, $a'\rho = a'$, $\zeta\rho = \zeta$, (2) $\lambda^m - a'$ _is irreducible in_ $A'[\lambda;\rho]$, (3) $\sigma'^{-1}\rho^{-1}\sigma'\rho = \widetilde{a''}$, (4) $N_R(a'';\sigma') = \zeta$, _and_ (5) $a'\sigma' = a' \cdot a''\rho^{m-1} \cdot \ldots \cdot a''\rho \cdot a''$.

Amitsur [1]; Kishimoto [2], [3]; Tominaga [12].

16. Outer Galois theory and related results

Throughout the present section, we assume always B <u>is a simple</u> ring. A subgroup $\mathfrak{H}$ of $\mathfrak{G}$ is said to be <u>locally finite</u> if $\#\{a\mathfrak{H}\}$ is finite for every a in A, and $\mathfrak{H}$ is defined to be <u>almost outer</u> if $\mathfrak{H}$ contains only a finite number of inner automorphisms.

Proposition 16.1. <u>Let</u> B <u>be a regular subring of</u> A, <u>and</u> $\mathfrak{H}$ <u>a subgroup of</u> $\mathfrak{G}$ <u>containing</u> $\tilde{V}$.

(a) <u>If</u> $\mathfrak{H}$ <u>is locally finite then</u> $\mathfrak{H}$ <u>is almost outer, or what is the same,</u> V <u>is finite or coincides with</u> C, <u>and the converse is true provided</u> A/B <u>is left algebraic</u>.

(b) <u>If</u> $J(\mathfrak{H}) = B$ <u>and</u> $\mathfrak{H}$ <u>is locally finite, then</u> A/B <u>is (two-sided) locally finite</u>.

<u>Proof</u>. (a) If $\mathfrak{H}$ is almost outer then $(V^{\cdot}:C^{\cdot}) = \#\tilde{V} < \infty$, and hence $\#V < \infty$ or $V = C$ by Lemma 3.9. The first half is now an easy consequence of Prop. 3.10. Next, assume that $\mathfrak{H}$ is almost outer and A/B is left algebraic. By Cor. 8.5, there exists then some $B' = \sum_1^n D'e'_{ij} \in \mathcal{R}^{o}_{l.f}$ such that $V_A(\{e'_{ij}\})/D'$ is left algebraic. Given $d \in V_A(\{e'_{ij}\})$, we set $B'' = B'[d]$ $(\in \mathcal{R}^{o}_{l.f})$. Then, by Prop. 5.7, there holds $B''|\mathfrak{H} = \bigcup_1^s (B''|\sigma_i\tilde{V})$ with some $\sigma_i \in \mathfrak{H}$. And so, it follows at once $\#\{(de'_{ij})\mathfrak{H}\} \leqslant \#(B''|\mathfrak{H}) < \infty$, which means the local finiteness of .

(b) By (a), there holds $\#V < \infty$ or $V = C$. For an arbitrary finite subset F of A, consider the subring $T = B[\{E, F, V\}\mathfrak{H}]$ or $T = B[\{E, F\}\mathfrak{H}]$ according as $\#V < \infty$ or $V = C$, and set $T_o = V_T(E)$. If T^*_o is the division subring of D generated by T_o then $T^* = T^*_o[E]$ is a simple subring of A containing T. To be easily seen, T^* is the least subring of A containing T with the property that if t is an element of $T^* \cap A^{\cdot}$ then t^{-1} is contained in T^*, that is, T^* is the subring of A generated by T permitting to adjoin their inverses together with units. Then, T^* is evidently $\mathfrak{H}$-invariant, and hence $T^*|\mathfrak{H}$ is an automorphism group of T^*. Since

$T^*|\mathfrak{H}$ is finite and $I(T^*|\mathfrak{H}) = V$ or $V_{T^*}(T^*)$ according as $\#V < \infty$ or $V = C$, $T^*|\mathfrak{H}$ is an F-group of T^* with $B = J(T^*|\mathfrak{H})$. It follows then $[T^*:B] < \infty$ (§ 7), which proves our assertion that A/B is locally finite.

Now, on the group $\mathfrak{G}$ we place the finite topology (§ 1): The collection of sets $U(\sigma, F) = \{\tau \in \mathfrak{G}\ ;\ F|\tau = F|\sigma\}$ where F ranges over all the finite subsets of A (or subrings of A finitely generated over B as ring) and $\sigma \in \mathfrak{G}$ is a basis for the open sets. Then, $\mathfrak{G}$ is a Hausdorff space and $U(\sigma, F) = \mathfrak{G}(F)\sigma$. In particular, $\mathfrak{G}(T)$ is closed for every subset T of A. Moreover, $\mathfrak{G}$ is a totally disconnected topological group.

Proposition 16.2. *If $\mathfrak{G}$ is compact then it is locally finite, and conversely. In particular, if A/B is Galois then the following conditions are equivalent: (1) $\mathfrak{G}$ is compact, (2) $\mathfrak{G}$ is locally finite, and (3) A/B is left algebraic and $\mathfrak{G}$ is almost outer.*

Proof. For any $a \in A$ we have $\mathfrak{G} = \bigcup_\lambda \mathfrak{G}(\{a\})\sigma_\lambda$ where $\{\sigma_\lambda\ ;\ \lambda \in \Lambda\}$ is a complete representative system of $\mathfrak{G}$ modulo $\mathfrak{G}(\{a\})$. However, as $\mathfrak{G}$ is compact and every $\mathfrak{G}(\{a\})\sigma_\lambda$ is open, Λ has to be finite. Accordingly, $a\mathfrak{G} = \{a\sigma_\lambda\ ;\lambda \in \Lambda\}$ is finite. Conversely, assume that $\mathfrak{G}$ is locally finite. Then, $A = \bigcup_\lambda B[F_\lambda\mathfrak{G}]$ where F_λ ranges over all the finite subsets of A. Obviously, every $B[F_\lambda\mathfrak{G}]$ is $\mathfrak{G}$-invariant and the system $\{B[F_\lambda\mathfrak{G}]\}$ is directed. We set here $\mathfrak{G}_\lambda = B[F_\lambda\mathfrak{G}]|\mathfrak{G}$, that is a finite group. Then the topological group $\mathfrak{G}$ may be regarded as the inverse limit of the system $\{\mathfrak{G}_\lambda\}$, where $\lambda \geqslant \mu$ is defined to be $B[F_\lambda\mathfrak{G}] \supset B[F_\mu\mathfrak{G}]$ and the projection π_μ^λ is the contraction of $\mathfrak{G}_\lambda$ to $B[F_\mu\mathfrak{G}]$. Hence, $\mathfrak{G}$ is compact by Prop. 1.1. The final equivalences are now evident by Prop. 16.1.

Needless to say, $\mathfrak{G}$ is locally compact if and only if there exists a finite subset F of A such that $\mathfrak{G}(F) = \mathfrak{G}(B[F])$ is compact. Moreover, we can prove the next:

Proposition 16.3. *Let A be left locally finite over a regular subring B. If $\mathfrak{G}$ is locally compact then $[V:C] < \infty$, and conversely.*

Proof. There exists a finite subset F of A such that $\mathfrak{G}(F)$ is compact. Here, without loss of generality, we may assume that $B' = B[F]$ is in $\mathfrak{L}^{\circ}_{l.f}$. By Props. 16.1 and 16.2, it follows that $\# V_A(B') < \infty$ or $V_A(B') = C$. Hence, in any rate, there holds $[V_A(B'):C] < \infty$. On the other hand, by Prop. 5.4, $[V:V_A(B')]_R \leqslant [B':B]_L < \infty$. Consequently, we obtain $[V:C] < \infty$. Next, we shall prove the converse. As $[A:H] = [V:C] < \infty$ (Th. 7.7), we can find a finite subset F of A such that $B' = B[F]$ is a simple ring with $V_A(B') = C$. Then, noting that A/B' is left locally finite, the compactness of $\mathfrak{G}(B') = \mathfrak{G}(F)$ is a consequence of Props. 16.1 and 16.2.

Now, let $\mathfrak{H}$ be a non-empty subset of $\mathfrak{G}$. If $[B[F\mathfrak{H}]:B]_L < \infty$ for every finite subset F of A then we say that $(\mathfrak{H}, A/B)$ is locally finite dimensional (abbr. l.f.d.). In particular, if $(\mathfrak{G}, A/B)$ is l.f.d., we say simply $\mathfrak{G}$ is l.f.d. In case a field A is algebraic and Galois over B, it is well known that $\mathfrak{G}$ is l.f.d. More generally, if A/B is Galois and $\mathfrak{G}$ is locally finite then $\mathfrak{G}$ is l.f.d. by Prop. 16.1.

Proposition 16.4. Let A be left locally finite over a regular subring B. Then the following conditions are equivalent: (1) $\mathfrak{G}$ is l.f.d., (2) $(\tilde{V}, A/B)$ is l.f.d., and (3) $V = C$ or $[V:Z] < \infty$.

Proof. It suffices to prove (2) $\Longrightarrow$ (3) $\Longrightarrow$ (1). Firstly, assume that $(\tilde{V}, A/B)$ is l.f.d. and $V \neq C$. Then, for any element $a \in A \setminus H$, $T = B[\{E, a\}\tilde{V}]$ is left finite over B. If V is finite, then $[B\cdot V:B]_L < \infty$ trivially. On the other hand, if V is infinite then $V \subset T$ by Prop. 8.10. Hence, we obtain $[B\cdot V:B]_L < \infty$. Recalling here that $B\cdot V = B \otimes_Z V$, we see that $[V:Z] < \infty$ in either case. Next, assume that $V = C$ or $[V:Z] < \infty$. Then, by Prop. 16.1, we may restrict our attention to the case $[V:Z] < \infty$. As $[B\cdot V:B] = [V:Z] < \infty$, for given finite subset F of A the subring $T = B[F, V, E]$ is left finite over B. By Prop. 5.7, we have then $T|\mathfrak{G} = \cup_1^t (T|\sigma_i)\tilde{V}$ with some $\sigma_i \in \mathfrak{G}$. Hence, $B[F\mathfrak{G}] \subset B[F\sigma_1, \dots, F\sigma_t, V] \subset T[F\sigma_1, \dots, F\sigma_t]$, and hence $[B[F\mathfrak{G}]:B]_L \leqslant [T[F\sigma_1, \dots, F\sigma_t]:B]_L < \infty$, which means that $\mathfrak{G}$ is l.f.d.

If A/B if Galois with a Galois group $\mathfrak{G}'$ and $(\mathfrak{G}', A/B)$ is l.f.d., then for every finite subset F of A there exists some $N \in \mathfrak{R}_{l.f}/B[F]$ such that N/B is Galois with a Galois group contained in $N \mid \mathfrak{G}'$, and particularly in case $\mathfrak{G}'$ is regular, namely, in case $\widetilde{V} \subset \mathfrak{G}'$, the Galois group $\mathfrak{G}(N/B)$ is necessarily contained in $N \mid \mathfrak{G}'$ (Prop. 7.1). In general (without the assumption that A/B is Galois), if $\mathfrak{H}$ is a subset of $\mathfrak{G}$ and if for every finite subset F of A there exists some $N \in \mathfrak{R}_{l.f}/B[F]$ such that N/B is Galois and $\mathfrak{G}(N/B) \subset N|\mathfrak{H}$, then A/B is called $\mathfrak{H}$-<u>locally Galois</u>. Particularly, in case $\mathfrak{H}$ is a group containing $\widetilde{V}$, to be easily seen, A/B is $\mathfrak{H}$-locally Galois if and only if for every finite subset F of A there exists some $N \in \mathfrak{R}_{l.f}/B[F]$ such that N/B is Galois with a Galois group contained in $N|\mathfrak{H}$. Given a finite subset F of A, an intermediate ring N of A/B[F] is called an A/B-<u>shade</u> of F (or of B[F]) if N is Galois and finite over B and A is N-A-irreducible. Any A/B-shade is in $\mathfrak{R}_{l.f}$. A/B is called <u>locally Galois</u> if for every finite subset F of A there exists a simple subring N of A containing B[F] such that N/B is finite Galois, or what is the same, if every finite subset of A possesses its A/B-shade. Given a subset $\mathfrak{H}$ of $\mathfrak{G}$ and a finite subset F of A, an A/B-shade N of F is called an $\mathfrak{H}$-<u>shade</u> of F (or of B[F]) if $\mathfrak{G}(N/B)$ is contained in $N|\mathfrak{H}$. Needless to say, A/B is $\mathfrak{H}$-locally Galois if and only if every finite subset of A possesses its $\mathfrak{H}$-shade, and further we may remark that in case A/B is $\mathfrak{G}$-locally Galois every A/B-shade is necessarily a $\mathfrak{G}$-shade (Th. 7.2). If A/B is $\mathfrak{G}$-locally Galois then A/B is h-Galois (Prop. 7.1), and so Galois by Cor. 6.10.

Now, we shall establish the Galois theory for outer case, which will play always an essential role in the subsequent study. Assume that A is outer Galois and left algebraic over B with a Galois group $\mathfrak{H}$. By Props. 16.1 and 16.4, $\mathfrak{G}$ is l.f.d., and hence A/B is h-Galois. Accordingly, every intermediate ring of A/B is simple by Cor. 6.2. Next, we shall prove that $A'A'' = A''A'$ for intermediate rings A' and A'' of A/B. To see this, we set $\mathfrak{G}' = \mathfrak{G}(A')$, $\mathfrak{G}'' = \mathfrak{G}(A'')$ and X =

$J(\mathfrak{G}' \cap \mathfrak{G}'')$. Evidently, it suffices to prove our assertion for the case $[A:B] < \infty$. Take an element a in A such that $T_{\mathfrak{G}' \cap \mathfrak{G}''}(a) = 1$ (Th. 7.4 and Cor. 9.9). By Prop. 9.6, there exist $x_1, \ldots, x_t$, $y_1, \ldots, y_t \in A$ such that $\sum_i y_i\sigma \cdot x_i = \delta_{1\sigma}$ $(\sigma \in \mathfrak{G})$. If x is in X then $A'A''$ contains $\sum_i T_{\mathfrak{G}'}(xay_i) \cdot T_{\mathfrak{G}''}(x_i) =$ $\sum_{\sigma \in \mathfrak{G}'} \sum_{\tau \in \mathfrak{G}''} \sum_i (xa)\sigma \cdot y_i\sigma \cdot x_i\tau = T_{\mathfrak{G}' \cap \mathfrak{G}''}(xa) = x$, namely, $A'A'' \supset X$. Since $A'A''$ is evidently contained in X, we obtain $A'A'' = X$, and symmetrically $A''A' = X$. If B' is an arbitrary intermediate ring of A/B with $[B':B]_L < \infty$, then $J(\mathfrak{G}(B')) = B'$ (Cor. 6.10) and $B' = B[b']$ with some $b' \in B'$ (Th. 12.4). Since A is B'-A-irreducible (Th. 6.1), $\mathrm{Hom}({}_BB', {}_BA) = (B'|\mathfrak{G})A_R = \bigoplus_1^s (B'|\sigma_i)A_R$ with some $\sigma_i \in \mathfrak{G}$ and $B'|\mathfrak{G} = \{B'|\sigma_1, \ldots, B'|\sigma_s\}$ (Props. 7.1 and 5.7). Hence, $\#\{b'\mathfrak{G}\} = \#\{B'|\mathfrak{G}\} = s = [\mathrm{Hom}({}_BB', {}_BA):A_R]_R = [B':B]$, and $\mathrm{Cl}\,\mathfrak{G} = \mathfrak{G}$. If A' is an arbitrary (regular) intermediate ring of A/B then $A' = \bigcup B_\lambda$, where B_λ ranges over all the intermediate rings of A'/B with $[B_\lambda:B] < \infty$. For any a in $A\backslash A'$, $\mathfrak{M}_\lambda = \{\sigma \in \mathfrak{G}(B_\lambda);\ a\sigma \neq a\}$ is a non-empty closed subset of $\mathfrak{G}$ by the above remark $J(\mathfrak{G}(B')) = B'$, and $\{\mathfrak{M}_\lambda\}$ possesses the finite intersection property. Hence, $\mathfrak{G}$ being compact by Prop. 16.2, it follows that $\cap \mathfrak{M}_\lambda$ $(\subset \mathfrak{G}(A'))$ contains an element τ with $a\tau \neq a$, which proves $J(\mathfrak{G}(A')) = A'$. As $\mathfrak{G}(A')$ is locally finite obviously, A/A' is still locally finite (Prop. 16.1). Next, let ρ be an element of $\Gamma(A', A; B)$. By Cor. 6.10, the set $\mathfrak{N}_\lambda$ of all the extensions of $B_\lambda|\rho$ to automorphisms of A is a non-empty closed subset of the compact group $\mathfrak{G}$, and $\{\mathfrak{N}_\lambda\}$ possesses the finite intersection property. Hence, $\cap \mathfrak{N}_\lambda$ is non-empty, whence it follows that ρ is contained in $A'|\mathfrak{G}$. If A'/B is Galois then $\mathfrak{G}(A') \subset \mathfrak{G}' = \{\sigma \in \mathfrak{G};\ A'\sigma = A'\}$ and $A'|\mathfrak{G}' = \mathfrak{G}(A'/B)$ by the above, and so $J(\mathfrak{G}') = B$. Hence, $\mathfrak{G}'$ is dense in $\mathfrak{G}$, whence we see that A' is $\mathfrak{G}$-invariant.

Summarizing the facts obtained above, we state the following:

Theorem 16.5. *Assume that* A *is outer Galois and left algebraic over* B. *Let* A' *be an intermediate ring of* A/B, *and* $\mathfrak{G}$ *a Galois group of* A/B.

(a) A' *is simple*, A/A' *is locally finite*, $A'A'' = A''A'$ *for every intermediate ring* A'' *of* A/B, *and each* B-*ring isomorphism of* A' *into* A *can be extended to an element of* $\mathfrak{G}$.

(b) A/B *is h-Galois and there exists a* 1-1 *dual correspondence between closed subgroups of* $\mathfrak{G}$ *and intermediate rings of* A/B, *in the usual sense of Galois theory*.

(c) *If* $[A':B]_L < \infty$ *then there exists an element* $a' \in A'$ *such that* $A' = B[a']$, *and there holds* $\#(A'|\mathfrak{G}) = \#\{a'\mathfrak{G}\} = [A':B]$. *Conversely, if* $\#(A'|\mathfrak{G}) < \infty$ *then* $[A':B] < \infty$.

(d) *If* A'/B *is Galois then* A' *is* $\mathfrak{G}$-*invariant, and conversely*.

If A is $H\cdot V$-A-irreducible and H is B-H-irreducible then A is $B\cdot V$-A-irreducible (and conversely). In fact, for any non-zero element $a \in A$, $M = BVaA$ is a direct summand of the V-A-completely reducible module A: $A = M \oplus M'$ (Prop. 5.4). If $1 = e + e'$ ($e \in M$, $e' \in M'$) then e is evidently a non-zero element of H, and so $M \supset BeH = H \ni 1$, which means $M = A$. By the aid of this remark, we can prove the following:

Corollary 16.6. (a) *Let* A *be* $H\cdot V$-A-*irreducible*. *If* A/B *is Galois and* H/B *is left algebraic then* A/B *is h-Galois*.

(b) *Let* A *be Galois and left locally finite over* B. *If* $\mathfrak{G}$ *is discrete then* $[A:B] < \infty$, *and conversely*.

Proof. (a) Since H/B is outer Galois (Prop. 5.4) and left algebraic, H/B is locally finite and h-Galois (Th. 16.5). Hence, H is B-H-irreducible (Th. 6.1), and so A is $B\cdot V$-A-irreducible by the above remark. Our assertion is now a consequence of Cor. 5.6 (b).

(b) As $\mathfrak{G}$ is locally compact, $[V:C] < \infty$ by Prop. 16.3, and so A is Galois and finite over H. Since A is $H\cdot V$-A-irreducible (Th. 6.1), A/B is h-Galois by (a). Take a $B' \in \mathfrak{L}_{l.f}$ such that $\mathfrak{G}(B') = \{1\}$. Then, $A = J(\mathfrak{G}(B')) = B'$ by Cor. 6.10. The converse is trivial.

The next proposition will be often of use.

Proposition 16.7. *Let* A *be Galois over* B *with a regular Galois group* $\mathfrak{G}$, *and* H *a simple ring left algebraic over* B. *Let* T *be an intermediate ring of* A/B *such that* $[T:B]_L < \infty$ *and* A *is* T-A-*irreducible*.

(a) *If* $T' = J(\mathfrak{G}(T))$ *then* $[T' \cap H:B] < \infty$.

(b) *If* $[T:T \cap H]_L = [V:V_A(T)]_R$ *then* $\mathrm{Hom}({}_BT, {}_BA) = (T|\mathfrak{G})A_R$ *and* $T|\mathfrak{G} = T|\mathfrak{J}$.

Proof. (a) As was noted in the proof of Prop. 6.11, there holds $(T'|\mathfrak{G})A_R = \oplus_1^t (T'|\sigma_i\tilde{V})A_R$ with some $\sigma_i \in \mathfrak{G}$, whence it follows $T'|\mathfrak{G} = \cup_1^t (T'|\sigma_i\tilde{V})$ by Prop. 5.7. We obtain therefore $\infty > t \geqslant \#(T' \cap H|(T'|\mathfrak{G})) = \#(T' \cap H|(H|\mathfrak{G}))$. Noting that H is outer Galois and locally finite over B with a Galois group $H|\mathfrak{G}$ (Prop. 16.1), Th. 16.5 (c) yields that $[T' \cap H:B] < \infty$.

(b) $H' = T \cap H$ is simple and H is H'-H-irreducible (Ths. 16.5 and 6.1). Accordingly, as in the proof of Th. 16.5, we obtain $\mathrm{Hom}({}_BH', {}_BH) = (H'|\mathfrak{G})H_R = \oplus_1^s (H'|\sigma_i)H_R$ with some $\sigma_i \in \mathfrak{G}$. As $H'|\sigma_i \neq H'|\sigma_j$ for $i \neq j$, $(T|\sigma_i)A_R$ is not T_R-A_R-isomorphic to $(T|\sigma_j)A_R$ (Prop. 5.7). Hence, there holds $\sum_1^s (T|\sigma_i\tilde{V})A_R = \oplus_1^s (T|\sigma_i\tilde{V})A_R$ (Prop. 5.7), and so we have $[\sum_1^s (T|\sigma_i\tilde{V})A_R:A_R]_R = s\cdot[V:V_A(T)]_R = [\mathrm{Hom}({}_BH', {}_BH):H_R]_R\cdot[V:V_A(T)]_R = [H':B]_L\cdot[T:H']_L = [T:B]_L$ (Lemma 5.1 (d)), which means $\mathrm{Hom}({}_BT, {}_BA) = \sum_1^s (T|\sigma_i\tilde{V})A_R = (T|\mathfrak{G})A_R$. Now, $T|\mathfrak{G} = T|\mathfrak{J}$ is also evident by Prop. 5.7.

Jacobson [6]; Krull [1]; Miyashita [2]; Nagahara-Tominaga [1], [2], [3], [4], [6], [8], [9]; Nobusawa [1], [2], [3]; Tominaga [2], [3].

17. q-system

Throughout the present section, we assume again B <u>is a simple ring</u>. Let T be in $\mathcal{R}^{o}$. A subset $\mathfrak{H}$ of $\mathfrak{G}(T, A; B)$ is called a <u>$\tilde{V}$-subset</u> of $\mathfrak{G}(T, A; B)$ if $\mathfrak{H}\tilde{V} = \mathfrak{H}$. If σ_1, σ_2 are in $\mathfrak{G}(T, A; B)$ and $\sigma_1 = \sigma_2\tilde{v}$ for some $v \in V^{\cdot}$ then we write $\sigma_1 \sim \sigma_2$. Evidently, $\sim$ is an equivalence relation in $\mathfrak{G}(T, A; B)$. Then, for any $\tilde{V}$-subset $\mathfrak{H}$ of $\mathfrak{G}(T, A; B)$ we denote by $(\mathfrak{H}:\tilde{V})$ the uniquely determined number of equivalence classes of $\mathfrak{H}$ with respect to $\sim$. If $\mathfrak{H} = \bigcup_{i\in I} \sigma_i\tilde{V}$ (direct union), then $\mathfrak{H}A_R = \oplus_{i\in I} \sigma_i\tilde{V}A_R$ is the idealistic decomposition of the T_R-A_R-module $\mathfrak{H}A_R$ (Prop. 5.7). In particular, if T is in $\mathcal{R}^{o}_{l.f}$ then $(\mathfrak{G}(T, A; B):\tilde{V}) \leqslant [T:B]_L < \infty$.

A <u>left</u> q_o-<u>system</u> $\mathcal{H} = \{\mathfrak{H}_T\}$ of A/B is defined as a function which attaches to each $T \in \mathcal{R}^{o}_{l.f}$ a non-empty $\tilde{V}$-subset $\mathfrak{H}_T$ of $\mathfrak{G}(T, A; B)$ such that $\sigma\mathfrak{H}_{T\sigma} \subset \mathfrak{H}_T$ for every $\sigma \in \mathfrak{H}_T$. Obviously, $\mathcal{G} = \{\mathfrak{G}_T = \mathfrak{G}(T, A; B)\}$ is a left q_o-system of A/B and there holds $\sigma\mathfrak{G}_{T\sigma} = \mathfrak{G}_T$ for every σ in $\mathfrak{G}_T$.

Lemma 17.1. <u>Let</u> $\mathcal{H} = \{\mathfrak{H}_T\}$ <u>be a left q_o-system of</u> A/B.

(a) <u>If</u> T' <u>is a member of</u> $\mathcal{R}^{o}_{l.f}$ <u>such that</u> $\tau'\mathfrak{H}_{T'\tau'} = \mathfrak{H}_{T'}$ <u>for every</u> $\tau' \in \mathfrak{H}_{T'}$ <u>then</u> $\mathfrak{H}_{T'\tau'}$ <u>contains</u> 1 <u>and</u> $\tau''\mathfrak{H}_{T'\tau'\tau''} = \mathfrak{H}_{T'\tau'}$ <u>for every</u> τ'' <u>in</u> $\mathfrak{H}_{T'\tau'}$.

(b) <u>For every</u> T <u>in</u> $\mathcal{R}^{o}_{l.f}$ <u>there exists some</u> $\sigma \in \mathfrak{H}_T$ <u>such that</u> $\mathfrak{H}_{T\sigma}$ <u>contains</u> 1 <u>and</u> $\tau\mathfrak{H}_{T\sigma\tau} = \mathfrak{H}_{T\sigma}$ <u>for every</u> τ <u>in</u> $\mathfrak{H}_{T\sigma}$.

<u>Proof</u>. (a) Since $\tau'\tau'' \in \mathfrak{H}_{T'}$ and $\tau''\mathfrak{H}_{T'\tau'\tau''} \subset \mathfrak{H}_{T'\tau'}$, we obtain $(\mathfrak{H}_{T'}:\tilde{V}) = (\tau'\mathfrak{H}_{T'\tau'}:\tilde{V}) = (\mathfrak{H}_{T'\tau'}:\tilde{V}) \geqslant (\tau''\mathfrak{H}_{T'\tau'\tau''}:\tilde{V}) = (\mathfrak{H}_{T'\tau'\tau''}:\tilde{V}) = (\mathfrak{H}_{T'}:\tilde{V})$. It follows therefore $(\mathfrak{H}_{T'\tau'}:\tilde{V}) = (\tau''\mathfrak{H}_{T'\tau'\tau''}:\tilde{V})$, and so $\tau''\mathfrak{H}_{T'\tau'\tau''} = \mathfrak{H}_{T'\tau'}$.

(b) Since $(\mathfrak{H}_{T\rho}:\tilde{V}) \leqslant [T\rho:B]_L = [T:B]_L$ for every ρ in $\mathfrak{H}_T$, we can find $\sigma' \in \mathfrak{H}_T$ such that $(\mathfrak{H}_{T\sigma'}:\tilde{V})$ is minimal. Then, for every

$\tau \in \mathfrak{H}_{T\sigma'}$ we obtain $(\tau\mathfrak{H}_{T\sigma'\tau}:\widetilde{V}) = (\mathfrak{H}_{T\sigma'\tau}:\widetilde{V}) \geqslant (\mathfrak{H}_{T\sigma'}:\widetilde{V})$. Combining this with $\tau\mathfrak{H}_{T\sigma'\tau} \subset \mathfrak{H}_{T\sigma'}$, we readily obtain $\tau\mathfrak{H}_{T\sigma'\tau} = \mathfrak{H}_{T\sigma'}$. Now, for an arbitrary $\sigma'' \in \mathfrak{H}_{T\sigma'}$ we set $\sigma = \sigma'\sigma''$. Then, by (a), $\mathfrak{H}_{T\sigma} = \mathfrak{H}_{T\sigma'\sigma''}$ contains 1 and $\tau\mathfrak{H}_{T\sigma\tau} = \mathfrak{H}_{T\sigma}$ for every $\tau \in \mathfrak{H}_{T\sigma}$.

A left q_o-system $\mathcal{H} = \{\mathfrak{H}_T\}$ of A/B is called a <u>left pre-q-system</u> if $T|\mathfrak{H}_{T'} = \mathfrak{H}_T$ for every $T' \in \mathcal{R}^{\circ}_{l.f}/T$, and a left pre-q-system $\mathcal{H} = \{\mathfrak{H}_T\}$ of A/B is called a <u>left q-system</u> if $J(\mathfrak{H}_T) = B$. In the obvious way, we can define a right pre-q-system and a right q-system. If A/B is w-q-Galois and left locally finite then $\mathcal{G}$ is a left q-system (Th. 6.5 and Lemma 6.8), and one will see later that $\mathcal{G}$ is the unqieu left q-system as well as the unique right q-system of A/B provided A/B is q-Galois and left locally finite.

Lemma 17.2. <u>Let</u> A <u>be left locally finite over</u> B, <u>and</u> $\mathcal{G} = \{\mathfrak{G}(T, A; B)\}$.

(a) <u>If</u> A/B <u>is w-q-Galois then</u> $\mathcal{G}$ <u>is a left q-system</u>.

(b) <u>Let</u> B' <u>be an intermediate ring of</u> A/B <u>such that</u> A <u>is</u> B'-A-<u>irreducible and</u> $[B':B]_L < \infty$, <u>and let</u> T <u>be in</u> $\mathcal{R}^{\circ}_{l.f}/B'$. <u>If</u> $\mathcal{G}$ <u>is a left pre-q-system then</u> $[V:V_A(B')]_R = [V:V_A(B'\sigma)]_R$ <u>for every</u> σ <u>in</u> $\mathfrak{G}(T, A; B)$.

<u>Proof</u>. It remains to prove (b). Let $\{v_1, \dots, v_t\}$ be a right $V_A(B')$-basis of V (Prop. 5.4), and T' in $\mathcal{R}^{\circ}_{l.f}/T[\{v_i\}]$. There exists then some $\sigma' \in \mathfrak{G}(T', A; B)$ such that $T|\sigma' = \sigma$. Assume that $\sum (B'\sigma|(v_i\sigma')_L)a_{iR} = 0$ ($a_i \in A$), or what is the same, $\sum (B'|\sigma(v_i\sigma')_L)a_{iR} = 0$, and take a $\sigma'' \in \mathfrak{G}((T'\sigma')[\{a_i\}], A; B)$ such that $\sigma'^{-1} = T'\sigma'|\sigma''$. Since $0 = (\sum (B'|\sigma(v_i\sigma')_L)a_{iR})\sigma'' = \sum (B'|v_{iL})(a_i\sigma'')_R$, it follows $a_i\sigma'' = 0$, namely, $a_i = 0$ (Prop. 5.1 (d)). Recalling that A is $B'\sigma$-A-irreducible by Prop. 5.1 (b), the above fact means that $\{v_1\sigma', \dots, v_t\sigma'\}$ is right free over $V_A(B'\sigma)$ (Prop. 5.1 (d)). It follows therefore $[V:V_A(B')]_R \leqslant [V:V_A(B'\sigma)]_R$, and symmetrically the converse inequality.

Lemma 17.3. <u>Let</u> $B \subset C$, <u>and let</u> A <u>be locally finite over</u> B. <u>If</u> $J(\mathfrak{G}(T, A; B)) = B$ <u>for every</u> $T \in \mathfrak{R}^{\circ}_{l.f}$ <u>then</u> A/B <u>is q-Galois</u>.

<u>Proof</u>. Let T be in $\mathfrak{R}^{\circ}_{l.f}$. First, we shall show that for every every $a \in A$ and $t_1, t_2 \in T$ such that $\{t_1, t_2\}$ is B-free and $t_1 \in T^{\cdot}$ there exists some $\xi \in \mathfrak{G}(T, A; B)A_R$ such that $t_1\xi = 0$ and $t_2\xi = a$. Since $t_2t_1^{-1} \in T\backslash B$, there exists some $\rho \in \mathfrak{G}(T, A; B)$ such that $(t_2t_1^{-1})\rho \neq t_2t_1^{-1}$, and then for $\eta = 1 - \rho(t_1\rho)_R^{-1}t_{1R} \in \mathfrak{G}(T, A; B)A_R$ we have $t_1\eta = 0$ and $t_2\eta \neq 0$. Noting that A is $\tilde{A}A_R$-irreducible, we can find then some $\xi \in \eta\tilde{A}A_R = \eta\tilde{V}A_R \subset \mathfrak{G}(T, A; B)A_R$ such that $t_2\xi = a$. Now, we shall prove our lemma. To our end, it will suffice to show that for every $a \in A$ and $x_1, \dots, x_m \in T^{\cdot}$ such that $\{x_1, \dots, x_m\}$ is B-free there exists an element $\xi \in \mathfrak{G}(T, A; B)A_R$ such that $x_i\xi = 0$ for every $i \neq m$ and $x_m\xi = a$. For $m = 2$, our assertion holds good by the above remark. Assume that we can find $\xi_1, \dots, \xi_{m-1} \in \mathfrak{G}(T, A; B)A_R$ such that $x_i\xi_j = \delta_{ij}x_i$ $(i, j = 1, \dots, m - 1)$. There holds then $x_i(\sum_1^{m-1} \xi_j - 1) = 0$ for $i = 1, \dots, m$. If $x_m(\sum \xi_j - 1) \neq 0$ then $x_m(\sum \xi_j - 1)\tilde{A}A_R = A$, and our assertion holds for some $\xi \in (\sum \xi_j - 1)\tilde{A}A_R \subset \mathfrak{G}(T, A; B)A_R$. If otherwise $x_m = \sum_1^{m-1} x_m\xi_j$ then, say, $\{x_1, x_m\xi_1\}$ is B-free. We set here $\xi_1 = \sum_1^k \rho_p a_{pR}$ where $\rho_p \in \mathfrak{G}(T, A; B)$ and $a_p \in A$. If $T' = T[\bigcup T\rho_p, \{a_p\}]$ then by the remark stated at the opening there exists an element $\xi' \in \mathfrak{G}(T', A; B)A_R$ such that $x_1\xi' = 0$ and $x_m\xi_1\xi' = a$. Now, it will be easy to see that $x_i\xi_1\xi' = 0$ for $i = 1, \dots, m - 1$, and hence $\xi = \xi_1\xi' \in \mathfrak{G}(T, A; B)A_R$ is an element requested.

Corollary 17.4. <u>Let</u> A <u>be left locally finite over a regular subring</u> B. <u>If</u> $\mathcal{H} = \{\mathfrak{h}_T\}$ <u>is a left q-system of</u> A/B <u>then</u> V <u>is locally finite and q-Galois over</u> Z <u>and</u> $(T \cap C_o)\mathfrak{h}_T \subset C_o$ <u>for every</u> $T \in \mathfrak{R}^{\circ}_{l.f}$.

<u>Proof</u>. Since $B \cdot V = B \otimes_Z V$, V/Z is locally finite. Moreover, noting that $(T \cap V)\mathfrak{h}_T \subset V$, one will easily see that $J(\mathfrak{G}(V', V; Z)) = Z$ for every simple intermediate ring V' of V/Z with $[V':Z] < \infty$

and $|V'| = |V|$. Hence, V/Z is q-Galois by Lemma 17.3. Now, let T' be in $\mathfrak{R}^{o}_{l.f}/T[\Gamma]$. Then, $V' = T' \cap V$ is a simple intermediate ring of V/Z such that $[V':Z] < \infty$ and $|V'| = |V|$. Hence, $(T \cap C_o)\mathfrak{G}_T = (T \cap C_o)(T|\mathfrak{G}_{T'}) = (T \cap C_o)(V'|\mathfrak{G}_{T'}) \subset (T \cap C_o)\mathfrak{J}(V', V; Z) \subset (V' \cap C_o)\mathfrak{J}(V', V; Z) \subset C_o$ (Th. 6.5 (c)).

Lemma 17.5. *Let* A *be left locally finite over a regular subring* B. *Then*, A *is left locally finite over the simple ring* $B \cdot C_o$ *and* $[V_{B'[V]}(V):B \cdot C_o]_L < \infty$ *for every* $B' \in \mathfrak{R}^{o}_{l.f}$.

Proof. We set $V' = V_A(B')$, $Z' = V_{B'}(B')$ and $C'_o = V_{V'}(V')$. Since $[V:V']_L \leqslant [B':B]_L < \infty$ (Prop. 5.4), we set $V = \sum_1^p V'v_i$. Then, $B' \cdot V \subset V' \cdot B'[v_1, \ldots , v_p]$, and so one will easily see that $B'[V]$ $V' \cdot B'[v_1, \ldots , v_p]$. Hence, it follows $[B'[V]:B' \cdot V']_L < \infty$ (cf. Cor. 4.5). Combining this with $B' \cdot V' = B' \otimes_{Z'} V' \subset B' \cdot C'_o \otimes_{C'_o} V' \subset (B' \cdot C'_o)[V_{B'[V]}(V)] \otimes_{C'_o} V' \subset B'[V]$, it follows that $[(B' \cdot C'_o)[V_{B'[V]}(V)]:B' \cdot C'_o]_L < \infty$ (cf. Cor. 4.5). Moreover, we obtain $[B' \cdot C'_o:B' \cdot (C_o \cap C'_o)]_L \leqslant [C'_o:C_o \cap C'_o] = [V_{B'[V]}(B' \cdot V'):V_{B'[V]}(B'[V])] \leqslant [B'[V]:B' \cdot V']_L < \infty$ (Prop. 5.4). Combining those above, it follows $[(B' \cdot C'_o)[V_{B'[V]}(V)]:B \cdot (C_o \cap C'_o)]_L < \infty$ (cf. Prop. 4.5). Noting that $V_{B'[V]}(V) \supset B \cdot C_o \supset B \cdot (C_o \cap C'_o)$, the last implies $[V_{B'[V]}(V):B \cdot C_o]_L < \infty$. Finally, $[(B \cdot C_o)[B']:B \cdot C_o]_L = [B'[C_o]:B \cdot C_o]_L < \infty$ means obviously the left local finiteness of $A/B \cdot C_o$.

Lemma 17.6. *Assume that* A/B *is left locally finite*. *Let* S *be in* $\mathfrak{R}^{o}_{l.f}$, *and* $\mathfrak{J}(S, A; B)A_R = \sum_1^{s'} \sigma_p A_R$ $(\sigma_p \in \mathfrak{J}(S, A; B))$. *Then*, *for any finite subset* F *of* A, *there exists some* $T \in \mathfrak{R}^{o}_{l.f}/S[F]$ *such that* $\mathfrak{J}(S, A; B) = \bigcup_1^{s'} \sigma_p \tau \widetilde{V}$ *for every* $\tau \in \mathfrak{J}(T, A; B)$.

Proof. If β is in $\mathrm{Hom}({}_BS, {}_BA)$ then every $\beta(e_{ii}A)_R$ is either 0 or A_R-irreducible. Hence, it follows $\mathrm{Hom}({}_BS, {}_BA) = \mathfrak{J}(S, A; B)A_R \oplus (\oplus_1^{s''} \beta_q(e_qA)_R)$, where $\beta_q \in \mathrm{Hom}({}_BS, {}_BA)$ and $e_q \in E$. Now, let

$\{x_1, \dots, x_s\}$ be a left B-basis of S. Then, $\mathrm{Hom}({}_BS, {}_BA)$ possesses an A_R-basis $\{\alpha_1, \dots, \alpha_s\}$ such that $x_\lambda \alpha_\mu = \delta_{\lambda\mu}$ (Prop. 2.6). We set $\alpha_\mu = \sum \sigma_p x_{p\mu R} + \sum \beta_q e_{qR} y_{q\mu R}$, where $x_{p\mu}, y_{q\mu} \in A$. Now, choose an arbitrary $T \in \mathcal{R}^{\circ}_{l.f}/S[F, \cup S\sigma_p, \cup S\beta_q, \{x_{p\mu}\}, \{y_{q\mu}\}, E]$. Since $\alpha_\mu = \alpha_\mu \tau \in \sum_1^{s'} \sigma_p \tau A_R + \sum_1^{s''} \beta_q \tau (e_q \tau \cdot A)_R$, $\sum_1^{s'} \sigma_p \tau A_R \subset \mathcal{G}(S, A; B)A_R$ and $[\sum_1^{s''} \beta_q \tau (e_q \tau \cdot A)_R | A_R] \leq s''$ for every $\tau \in \mathcal{G}(T, A; B)$, one will readily see that $\mathcal{G}(S, A; B)A_R = \sum_1^{s'} \sigma_p \tau A_R$. Hence, our assertion is a consequence of Prop. 5.7.

Proposition 17.7. Let A be left locally finite over a regular subring B. If $\mathcal{H} = \{\mathcal{H}_T\}$ is a left q-system of A/B then $(T \cap H)\tau = T\tau \cap H$ for every $\tau \in \mathcal{H}_T$.

Proof. By Prop. 5.7, $\mathcal{G}(T, A; B) = \cup_1^t \tau_i \tilde{V}$ where $\tau_i \in \mathcal{G}(T, A; B)$. We set $B' = T[\cup_1^t T\tau_i]$ $(\in \mathcal{R}^{\circ}_{l.f})$ and $H' = V_{B'[V]}(V)$. Then, H' has a finite left $B \cdot C_o$-basis $\{h_1', \dots, h_m'\}$ (Lemma 17.5). Obviously, there exists a finite subset F of V such that $R = B'[F]$ contains $\{h_1', \dots, h_m'\}$. Now, let τ be an arbitrary element of $\mathcal{H}_T$. Then, $\tau = T|\rho$ for some $\rho \in \mathcal{H}_R$. By Lemma 17.6, there exists some $T' \in \mathcal{R}^{\circ}_{l.f}/R$ and $\tau' \in \mathcal{H}_{T'}$ such that $R|\tau' = \rho$ and $\rho'\tau' \sim 1$ for some $\rho' \in \mathcal{G}(R, A; B)$. Evidently, $V_R(V)\rho' \subset R\rho' \subset B'[V]$. If there exists some $h \in V_R(V)$ such that $h\rho' \notin H$, we can find some $u \in V$ with $h\rho' \cdot u \neq u \cdot h\rho'$. For an arbitrary $S \in \mathcal{R}^{\circ}_{l.f}/T'[u]$, there exists some $\sigma \in \mathcal{H}_S$ with $T'|\sigma = \tau'$. Then, noting that $V_R(V)|\rho'\tau' = 1$, we readily obtain $h \cdot u\sigma = (h\rho' \cdot u)\sigma \neq (u \cdot h\rho')\sigma = u\sigma \cdot h$, which is a contradiction. We have seen therefore that $V_R(V)\rho' \subset H'$. Accordingly, $h_j = h_j'\rho' \in H'$ and $h_j\tau' = h_j'$. Let F' be an arbitrary finite subset of C_o, and T'' in $\mathcal{R}^{\circ}_{l.f}/T'[F']$. Then, there exists some $\tau'' \in \mathcal{H}_{T''}$ with $T'|\tau'' = \tau'$, and $F'\tau'' \subset C_o$ by Cor. 17.4. Hence, noting that $\{h_j\tau'' = h_j' ; j = 1, \dots, m\}$ is left free over $B[F'\tau'']$ $(\subset B \cdot C_o)$, we see that $\{h_1, \dots, h_m\}$ is a left $B[F']$-basis of $\sum_1^m B[F']h_j$. Accordingly,

$\{h_1, \ldots, h_m\}$ is a left $B\cdot C_o$-basis of $\sum_1^m (B\cdot C_o)h_j$, namely, $H' = \oplus_1^m (B\cdot C_o)h_j$. We can choose then a finite subset F^* of C_o such that $T \cap H = V_T(V) \subset \sum_1^m B[F^*]h_j$. If T^* is in $\mathcal{L}^{\,o}_{1.f}/T'[F^*]$, there exists some $\tau^* \in \mathcal{G}_{T^*}$ such that $T'|\tau^* = \tau'$. It follows then $(T \cap H)\tau = (T \cap H)\tau^* \subset (\sum_1^m B[F^*]h_j)\tau^* = \sum_1^m B[F^*\tau^*]h_j' \subset H' \subset H$. Finally, we shall prove $T\tau \cap H \subset (T \cap H)\tau$. Let $h' = t\tau$ $(t \in T)$ be an element of $T\tau \cap H$. If t is not contained in H then there exists some $u' \in V$ such that $tu' \neq u't$. There exists a $\sigma' \in \mathcal{G}_{T[u']}$ such that $\tau = T|\sigma'$, and then $h'\cdot u'\sigma' = t\sigma'\cdot u'\sigma' \neq u'\sigma'\cdot t\sigma' = u'\sigma'\cdot h'$. This is a contradiction.

Lemma 17.8. <u>Let</u> A <u>be left locally finite over a regular subring</u> B, <u>and</u> H <u>a simple ring</u>. <u>If there exists a left</u> **<u>q-system</u>** $\mathcal{H} = \{\mathcal{G}_T\}$ <u>of</u> A/B <u>then</u> H/B <u>is outer Galois</u>, $T \cap H\,|\,\mathcal{G}_T = T \cap H|\,\mathfrak{G}(H/B) = \mathfrak{G}(T \cap H, H; B)$, <u>and</u> $\#(T \cap H\,|\,\mathcal{G}_T) = [T \cap H{:}B]$.

<u>Proof</u>. Let T_α be an arbitrary member of $\mathcal{L}^{\,o}_{1.f}$, and $H_\alpha = T_\alpha \cap H$. Since $H_\alpha \mathcal{G}_{T_\alpha} \subset H$ by Prop. 17.7, $\mathcal{G}^*_\alpha = H_\alpha|\mathcal{G}_{T_\alpha} \subset \Gamma(H_\alpha, H; B)$ and $\#\mathcal{G}^*_\alpha \leqslant (\mathcal{G}_{T_\alpha}{:}V) < \infty$. Obviously $A = \bigcup_{T_\alpha \in \mathcal{L}^{o}_{l.f}} T_\alpha$ yields $H = \bigcup H_\alpha$. If $T_\alpha \supset T_\beta$ then $T_\beta|\mathcal{G}_{T_\alpha} = \mathcal{G}_{T_\beta}$, and so $H_\beta|\mathcal{G}^*_\alpha = \mathcal{G}^*_\beta$. Hence, we can consider the inverse limit $\mathcal{G}^* = \varprojlim \mathcal{G}^*_\alpha$, that may be regarded as a subset of $\mathfrak{G}(H, H; B)$. Since every $\mathcal{G}^*_\alpha$ is finite, there holds then $H_\alpha|\mathcal{G}^* = \mathcal{G}^*_\alpha$ (Prop. 1.1). Combining this with $J(\mathcal{G}^*_\alpha) = J(\mathcal{G}_{T_\alpha}) \cap H = B$, we readily obtain $J(\mathcal{G}^*) = B$. Now, let σ^* and τ^* be in $\mathcal{G}^*$. Then, $H_\alpha|\sigma^* = H_\alpha|\sigma$ for some $\sigma \in \mathcal{G}_{T_\alpha}$, and $H_\alpha\sigma^*|\tau^* = (T_\alpha \cap H)\sigma|\tau^* = T_\alpha\sigma \cap H\,|\tau^* = T_\alpha\sigma \cap H|\tau$ for some $\tau \in \mathcal{G}_{T_\alpha\sigma}$ (Prop. 17.7). Hence, $H_\alpha\,|\sigma^*\tau^* = (H_\alpha|\sigma^*)\tau^* = H_\alpha|\sigma\tau \in \mathcal{G}^*_\alpha = H_\alpha|\mathcal{G}^*$, which means $H_\alpha|(\mathcal{G}^*)^2 \subset H_\alpha|\,\mathcal{G}^*$. Hence, we can find a positive integer n_α such that $H_\alpha|\sigma^{*n_\alpha} = 1$, which proves $H\sigma^* = H$, that is, σ^* is an automorphism of H. We have proves thus H/B is outer Galois. Recalling that $H_\alpha|(\mathcal{G}^*)^2 \subset H_\alpha\,|\mathcal{G}^*$, the rest of our assertion will be easily seen by Th. 16.5.

Lemma 17.9. *Let* H *be simple, and* T' *an intermediate ring of* $A/B[\Delta]$.

(a) *If there exists a subset* $\mathcal{G}$ *of* $\Gamma(H[T'], A; T')$ *such that* $J(\mathcal{G}) \cap H = T' \cap H$ *and* $H\mathcal{G} \subset H$, *and if* $T' \cap H$ *is simple then* T' *is linearly disjoint from* H, *namely, every right basis and left basis of* T' *over* $T' \cap H$ *are right and left* H*-free, respectively*.

(b) *Let* A *be left locally finite over a regular subring* B, *and* $[T':B]_L < \infty$. *If there exists a left q-system* $\mathcal{H} = \{\mathcal{G}_T\}$ *of* A/B *such that* $J(\mathcal{G}_{T''}(T')) \cap H = T' \cap H$ *for every* $T'' \in \mathcal{R}^{\circ}_{l.f}/T'$ *then* T' *is linearly disjoint from* H.

Proof. (a) We set $H' = T' \cap H = \sum K'd_{hk}$ with the subring $K' = V_{H'}(\Delta)$ of K. Suppose that a left basis $\{t_i;\ i \in I\}$ of T' over H' is not free over H. Then, every $d_{hk}t_i$ is non-zero and $\{d_{hk}t_i\}$ is not free over K. Here, without loss of generality, we may assume that $d_{11}t_1 = \sum a_{hki}d_{hk}t_i$ $(a_{hki} \in K)$ is a non-trivial relation of the shortest length. Then, some $a_{h'k'i'}$ does not belong to H', namely, $a_{h'k'i'}\sigma \neq a_{h'k'i'}$ for some $\sigma \in \mathcal{G}$, and so $0 = (d_{11}t_1)\sigma - d_{11}t_1 = \sum (a_{hki}\sigma - a_{hki})d_{hk}t_i$ $(a_{hki}\sigma \in K)$, which is a contradiction.

(b) Since H/B is outer Galois by Lemma 17.8, $T' \cap H$ is simple (Th. 16.5). Accordingly, by the validity of Prop. 17.7, our proof will proceed in the same way as in (a).

Lemma 17.10. *Let* A *be left locally finite over a regular subring* B, *and* H *a simple subring*. *Let* $\mathcal{H} = \{\mathcal{G}_T\}$ *be a left q-system of* A/B.

(a) *If* T' *is a member of* $\mathcal{R}^{\circ}_{l.f}$ *that is linearly disjoint from* H *then* $T'\tau'$ *is linearly disjoint from* H *for every* $\tau' \in \mathcal{G}_{T'}$.

(b) *If* T *is in* $\mathcal{R}^{\circ}_{l.f}$ *then there exists some* $T^* \in \mathcal{R}^{\circ}_{l.f}$ *such that* T^* *is linearly disjoint from* H *and* $T\tau^* \subset T^*$ *for some* $\tau^* \in \mathcal{G}_T$.

Proof. One may remark first that H/B is outer Galois (Lemma 17.8) and every intermediate ring of H/B is simple (Th. 16.5), and that $T\tau \cap H = (T \cap H)\tau$ for every $\tau \in \mathcal{G}_T$ (Prop. 17.7).

(a) Let $\{t_i\tau'\}$ be a right $(T'\tau' \cap H)$-basis of $T'\tau'$. Then, $\{t_i\}$ forms evidently a right $(T' \cap H)$-basis of T'. Assume that $\sum t_i\tau' \cdot h_i' = 0$ for some $h_i' \in H$. If N is an arbitrary $\mathfrak{G}(H/B)$-invariant shade of $\{h_i'\}$, and T'' in $\mathcal{R}^{\circ}_{1.f}/T'[N]$, then there exists $\tau'' \in \mathcal{G}_{T''}$ such that $T'|\tau'' = \tau'$. Since $N\tau'' = N$ by Th. 16.5, we can find some $\{h_i\} \subset N$ such that $h_i\tau'' = h_i'$. Hence, we obtain $0 = \sum t_i\tau' \cdot h_i\tau'' = (\sum t_ih_i)\tau''$, namely, $\sum t_ih_i = 0$. Recalling that T' is linearly disjoint from H, it follows then $h_i = 0$, and so $h_i' = 0$. This proves our assertion.

(b) By Lemma 17.1 (b), there exists some $\sigma \in \mathcal{G}_T$ such that $\mathcal{G}_{T\sigma}$ contains 1 and $\tau\mathcal{G}_{T\sigma\tau} = \mathcal{G}_{T\sigma}$ for every $\tau \in \mathcal{G}_{T\sigma}$. Therefore, to our end, it suffices to prove our assertion for $T \in \mathcal{R}^{\circ}_{1.f}/\Delta$ such that $\mathcal{G}_T \ni 1$ and $\tau\mathcal{G}_{T\tau} = \mathcal{G}_T$ for every $\tau \in \mathcal{G}_T$. We set here $\mathcal{S} = \{S \in \mathcal{R}^{\circ}_{1.f}/T;\ (\mathcal{G}_S:\widetilde{V}) = (\mathcal{G}_T:\widetilde{V})\}$. If S is in $\mathcal{S}$ then for every $\sigma \in \mathcal{G}_S$ we have $T|\sigma\mathcal{G}_S = (T|\sigma)\mathcal{G}_{T\sigma} = \mathcal{G}_T$. Accordingly, it follows $(\mathcal{G}_T:\widetilde{V}) = (T|\sigma\mathcal{G}_{S\sigma}:V) \leq (\sigma\mathcal{G}_{S\sigma}:\widetilde{V}) \leq (\mathcal{G}_S:\widetilde{V}) = (\mathcal{G}_T:\widetilde{V})$, which implies $(\mathcal{G}_{S\sigma}:\widetilde{V}) = (\sigma\mathcal{G}_{S\sigma}:\widetilde{V}) = (\mathcal{G}_S:\widetilde{V}) = (\mathcal{G}_T:\widetilde{V})$. Hence, we see that $\sigma\mathcal{G}_{S\sigma} = \mathcal{G}_S$ and $(\mathcal{G}_{S\sigma}:\widetilde{V}) = (\mathcal{G}_T:\widetilde{V})$, in particular, $S\sigma \in \mathcal{S}$ for every $\sigma \in \mathcal{G}_S$ with $T|\sigma = 1$. By Lemma 17.8, we have $[S \cap H:B] = \#(S \cap H|\mathcal{G}_S) \leq (\mathcal{G}_S:\widetilde{V}) = (\mathcal{G}_T:\widetilde{V})$ for every $S \in \mathcal{S}$. Hence, we can find a $T^* \in \mathcal{S}$ such that $[S \cap H:B] \leq [T^* \cap H:B]$ for every $S \in \mathcal{S}$. Since $[T^*\sigma \cap H:B] = [(T^* \cap H)\sigma:B] = [T^* \cap H:B]$ (Prop. 17.7) and $T^*\sigma \in \mathcal{S}$ for every $\sigma \in \mathcal{G}_{T^*}$ with $T|\sigma = 1$, we may assume that $\mathcal{G}_{T^*}$ contains 1 and $\tau\mathcal{G}_{T^*\tau} = \mathcal{G}_{T^*}$ for every $\tau \in \mathcal{G}_{T^*}$ (Lemma 17.1). Now, we shall prove that T^* is linearly disjoint from H. Let R be in $\mathcal{R}^{\circ}_{1.f}/T^*$, and set $R' = J(\mathcal{G}_R(T^*))$. Then, $R \supset R' \supset T^*$, and we have $\mathcal{G}_{T^*} = T^*|\mathcal{G}_R = \bigcup_1^m (T^*|\rho_i)\widetilde{V}$ (direct union) for some $\rho_i \in \mathcal{G}_R$. Let ρ be in $\mathcal{G}_R$. Then, $T^*|\rho = (T^*|\rho_k)\widetilde{v}$ with some ρ_k and $v \in V^{\cdot}$. Since $(T^*|\rho)\mathcal{G}_{T^*\rho} = \mathcal{G}_{T^*}$ contains 1, we can find $\tau^* \in \mathcal{G}_{T^*\rho}$ such that $(T^*|\rho)\tau^* = 1$. If $T' = R[R\rho, R\rho_k, v]$ $(\in \mathcal{R}^{\circ}_{1.f}/T^*\rho)$, then $\tau^* =$

$T^*\rho|\tau'$ for some $\tau' \in \mathfrak{G}_{T'}$, and then we have $T^*|1 = (T^*|\rho)\tau' = (T^*|\rho_k)\widetilde{v}\tau'$. Noting that $\rho\tau'$ and $\rho_k\widetilde{v}\tau'$ are in $\mathfrak{G}_R$, it follows then $R'|1 = (R'|\rho)\tau' = (R'|\rho_k)\widetilde{v}\tau'$. Thus, $R'|\rho = (R'|\rho_k)\widetilde{v}$, and hence $\mathfrak{G}_{R'} = R' \mid \mathfrak{G}_R = \bigcup_1^m (R'|\rho_i)\widetilde{V}$, which means $(\mathfrak{G}_{T^*}:\widetilde{V}) \geqslant (\mathfrak{G}_{R'}:\widetilde{V})$. Accordingly, $(\mathfrak{G}_{T^*}:\widetilde{V}) = (\mathfrak{G}_R:\widetilde{V})$, namely, $R' \in \mathcal{S}$. Then, there holds $[R' \cap H:B] \leqslant [T^* \cap H:B]$, whence it follows $R' \cap H = T^* \cap H$. Now, our assertion is a direct consequence of Lemma 17.9 (b).

We shall prove now the following:

Proposition 17.11. *Let* A *be left locally finite over* B, *and* $\mathcal{H} = \{\mathfrak{G}_T\}$ *a left q-system of* A/B.

(a) *The following conditions are equivalent*: (1) A/B *is q-Galois*, (2) A *is* $B \cdot V$-A-*irreducible*, (3) A *is* A-$B \cdot V$-*irreducible*, (4) B *and* H *are regular and* $[V_A^2(T):H]_L = [V:V_A(T)]_R$ *for every* $T \in \mathcal{R}_{l.f}^{\circ}$, *and* (5) B *and* H *are regular*, A/H *is left locally finite and* $[V_A^2(A'):H]_L = [V:V_A(A')]_R$ *for every* $A' \in \mathcal{R}^{\circ}/H$ *left finite over* H.

(b) *If any of the above equivalent conditions is satisfied, then* A/B *and* A/H *are (two-sided) locally finite (and so* $\mathcal{H}$ *is a right q-system of* A/B) *and* $\mathcal{H}$ *coincides with the left q-system* $\mathcal{G} = \{\mathfrak{g}(T, A; B)\}$.

Proof. Obviously, $(1) \Longrightarrow (2)$ by Th. 6.1. If any of the conditions (1) - (5) is satisfied then B and H are in $\mathcal{R}$ (Prop. 5.4), H/B is outer Galois (Lemma 17.8), and then for each $T \in \mathcal{R}_{l.f}^{\circ}$ there exists some $T^* \in \mathcal{R}_{l.f}^{\circ}$ such that T^* is linearly disjoint from H and $T\tau^* \subset T^*$ for some $\tau^* \in \mathfrak{G}_T$ (Lemma 17.10). We have then $[T^*:T^* \cap H]_L = [H \cdot T^*:H]_L \leqslant [V_A^2(T^*):H]_L$, $[T^*:T^* \cap H]_R = [T^* \cdot H:H]_R \leqslant [V_A^2(T^*):H]_R$. Moreover, by Prop. 5.4, we have $[V:V_A(T)]_L$ and $[V:V_A(T)]_R \leqslant [T:T \cap H]_L \leqslant [T:B]_L < \infty$, where $T \cap H$ is simple by Th. 16.5. $(3) \Longrightarrow (5) \Longrightarrow (4)$: The first implication is easy by Cor. 5.5, and the latter is obvious. $(4) \Longrightarrow (1)$: There holds $[T^*:T^* \cap H]_L \leqslant [V_A^2(T^*):H]_L = [V:V_A(T^*)]_R \leqslant [T^*:T^* \cap H]_L$, namely,

$[T^*:T^*\cap H]_L = [V:V_A(T^*)]_R$. If we set $T^*\cap H\,|\,\mathcal{G}_{T^*} = \{T^*\cap H|\sigma_1, \ldots, T^*\cap H|\sigma_m\}$ where $T^*\cap H|\sigma_i \neq T^*\cap H|\sigma_j$ for $i \neq j$ and $m = [T^*\cap H:B]$ (Lemma 17.8), then $\sigma_i A_R$ is not T^*_R-A_R-isomorphic to $\sigma_j A_R$ for $i \neq j$ (Props. 5.7 and 17.7). Hence, we have $\sum_1^m \sigma_i\tilde{V}A_R = \bigoplus_1^m \sigma_i\tilde{V}A_R$. Since every $T^*\sigma_i$ is linearly disjoint from H (Lemma 17.10 (a)), one may use $T^*\sigma_i$ instead of T^*. Accordingly, we obtain $[T^*\sigma_i:T^*\sigma_i\cap H]_L = [V:V_A(T^*\sigma_i)]_R$, and so $[V:V_A(T^*)]_R = [T^*:T^*\cap H]_L = [T^*\sigma_i:T^*\sigma_i\cap H]_L = [V:V_A(T^*\sigma_i)]_R$ (Prop. 17.7). Noting that V is generated by units, Prop. 5.1 (d) yields then $[\sigma_i\tilde{V}A_R:A_R]_R = [(T^*\sigma_i|\tilde{V})A_R:A_R]_R = [V:V_A(T^*\sigma_i)]_R = [V:V_A(T^*)]_R$, and then $[\bigoplus_1^m \sigma_i\tilde{V}A_R:A_R]_R = [T^*\cap H:B]\cdot[V:V_A(T^*)]_R = [T^*\cap H:B]\cdot[T^*:T^*\cap H]_L = [T^*:B]_L = [\mathrm{Hom}({}_BT^*, {}_BA):A_R]_R$. It follows therefore $\mathrm{Hom}({}_BT^*, {}_BA) = \mathcal{G}_{T^*}A_R$. Recalling here that $T\tau^* \subset T^*$, we see that $\mathrm{Hom}({}_BT\tau^*, {}_BA) = \mathcal{G}_{T\tau^*}A_R$. Hence, $\mathrm{Hom}({}_BT, {}_BA) = \tau^*\mathrm{Hom}({}_BT\tau^*, {}_BA) = \tau^*\mathcal{G}_{T\tau^*}A_R \subset \mathcal{G}_TA_R \subset \mathcal{J}(T, A; B)A_R \subset \mathrm{Hom}({}_BT, {}_BA)$. This implies that $\mathcal{G}_TA_R = \mathcal{J}(T, A; B)A_R = \mathrm{Hom}({}_BT, {}_BA)$ and $\mathcal{J}(T, A; B) = \mathcal{G}_T$ (Prop. 5.7). (2)$\Longrightarrow$(3): Since A is $B\cdot V$-A-irreducible, $\infty > [V:V_A(T^*)]_L \geqslant [V_A^2(T^*):H]_R \geqslant [T^*:T^*\cap H]_R$ (Prop. 5.4). Hence, by Lemma 17.8, $[T:B]_R = [T^*:B]_R \leqslant [T^*:T^*\cap H]_R\cdot[T^*\cap H:B] < \infty$, which means that A/B is right locally finite. Accordingly, $\mathcal{L}^{\circ}_{l.f} = \mathcal{R}^{\circ}_{r.f}$ and $\mathcal{H}$ is a right q-system of A/B, and hence it turns out that A is A-$B\cdot V$-irreducible symmetrically to (3)$\Longrightarrow$(4)$\Longrightarrow$(1)$\Longrightarrow$(2). Now, the rest of the proof will be evident by the above proof.

Corollary 17.12. <u>Let</u> A <u>be left locally finite over a regular subring</u> B.

(a) A/B <u>is h-Galois if and only if any of the following equivalent conditions is satisfied</u>: (H1) A/B <u>is Galois and q-Galois</u>, (H2) A/B <u>is Galois and</u> A <u>is</u> $B\cdot V$-A-<u>irreducible</u>, (H3) A/B <u>is Galois and</u> A <u>is</u>

A-B·V-<u>irreducible</u>, (H4) A/B <u>is Galois</u>, H <u>is simple and</u> $[V_A^2(T):H]_L = [V:V_A(T)]_R$ <u>for every</u> $T \in \mathfrak{K}^{\circ}_{l.f}$, <u>and</u> (H5) A/B' <u>is Galois for every</u> $B' \in \mathfrak{K}^{\circ}_{l.f}$, H <u>is simple and</u> $[V_A^2(A'):H]_L = [V:V_A(A')]_R$ <u>for every</u> $A' \in \mathfrak{K}\,?H$ <u>left finite over</u> H.

(b) <u>If</u> A/B <u>is h-Galois then</u> A/B <u>is locally finite and right h-Galois</u>.

<u>Proof</u>. If A/B is h-Galois then A/B' is Galois for every B' in $\mathfrak{K}_{l.f}$ (Cor. 6.10) and the conditions (H1) - (H5) are satisfied (Prop. 17.11). Conversely, if any of those conditions is satisfied then $\mathcal{G}(A/B) = \{ T \mid \mathfrak{G}(A/B)\}$ is obviously a left q-system of A/B. Hence, (H1) - (H4) are equivalent by Prop. 17.11, and then A/B is h-Galois. It remains therefore to prove (H5)$\Longrightarrow$(H1). Let T' be in $\mathfrak{K}^{\circ}_{l.f}/\Delta$, and N an arbitrary $\mathfrak{G}(H/B)$-invariant shade of $T' \cap H$. Then, $N[T'] | \mathfrak{G}(T')$ and $N | \mathfrak{G}(T')$ are outer Galois groups of $N[T']/T'$ and $N/T' \cap H$, repsectively. Since $[N:T' \cap H] = \#(N | \mathfrak{G}(T')) = \#(N[T'] | \mathfrak{G}(T')) = [N[T']:T']$ by Th. 16.5 (c), Lemma 17.9 (a) yields $[N \cdot T':N]_L = [T':T' \cap H]_L = [N[T']:N]_L$, whence we obtain $N \cdot T' = N[T']$. We readily see then $H \cdot T' = H[T']$ and $[H[T']:H]_L = [T':T' \cap H]_L < \infty$, which means that A/H is left locally finite. Hence, A/B is q-Galois by Prop. 17.11.

In the preceding section, we have noted that if A/B is $\mathfrak{G}$-locally Galois then it is Galois (and locally Galois). Conversely, if A/B is Galois and locally Galois then A/B is h-Galois by Cor. 17.12, and so for each A/B-shade B' we have $\mathfrak{G}(B'/B) \subset \mathfrak{G}(B', A; B) = B' | \mathfrak{G}$ (Cor. 6.10). Hence, we have the following:

Corollary 17.13. <u>In order that</u> A/B <u>be</u> $\mathfrak{G}$-<u>locally Galois, it is necessary and sufficient that</u> A/B <u>be Galois and locally Galois</u>.

Now, for every $T \in \mathfrak{K}^{\circ}_{l.f}$ we set $\hat{\mathfrak{G}}_T = \bigcap_{T' \in \mathfrak{K}^{\circ}_{l.f}/T} T | \mathfrak{G}(T', A; B)$. Obviously $\hat{\mathfrak{G}}_T$ is a $\tilde{V}$-subset of $\mathfrak{G}(T, A; B)$ and consists of all $\sigma \in \mathfrak{G}(T, A; B)$ such that for any $T' \in \mathfrak{K}^{\circ}_{l.f}/T$ there exists some $\sigma' \in \mathfrak{G}(T', A; B)$ such that $\sigma = T | \sigma'$.

Lemma 17.14. <u>Let</u> A <u>be left locally finite over</u> B.

(a) <u>If</u> T <u>is in</u> $\mathcal{R}^{\circ}_{1.f}$ <u>then there exists</u> $T^* \in \mathcal{R}^{\circ}_{1.f}/T$ <u>such that</u> $T|\mathcal{G}(T', A; B) = \hat{\mathcal{G}}_T$ <u>for every</u> $T' \in \mathcal{R}^{\circ}_{1.f}/T^*$.

(b) $\hat{\mathcal{G}} = \{\hat{\mathcal{G}}_T\}$ <u>is a left pre-q-system of</u> A/B.

<u>Proof</u>. (a) Since $(\mathcal{G}(T, A; B):\tilde{V}) < \infty$, there exist some $T_1, \dots, T_m \in \mathcal{R}^{\circ}_{1.f}/T$ such that $\hat{\mathcal{G}}_T = \bigcap_1^m T\,|\,\mathcal{G}(T_i, A; B)$. If $T^* = T[\bigcup_1^m T_i]$, then for every $T' \in \mathcal{R}^{\circ}_{1.f}/T^*$ we have $T\,|\,\mathcal{G}(T', A; B) = T|(T_i|\mathcal{G}(T', A; B)) \subset T|\mathcal{G}(T_i, A; B)$, and so $T|\mathcal{G}(T', A; B) \subset \bigcap_1^m T|\mathcal{G}(T_i, A; B) = \hat{\mathcal{G}}_T \subset T|\mathcal{G}(T', A; B)$.

(b) Let T' be in $\mathcal{R}^{\circ}_{1.f}/T$. By (a), we can find $T'' \in \mathcal{R}^{\circ}_{1.f}/T'$ such that $T|\mathcal{G}(T'', A; B) = \hat{\mathcal{G}}_T$ and $T'|\mathcal{G}(T'', A; B) = \hat{\mathcal{G}}_{T'}$. Hence, we have $T|\hat{\mathcal{G}}_{T'} = \hat{\mathcal{G}}_T$. Now, let σ be in $\hat{\mathcal{G}}_T$. Then, $\sigma = T|\sigma'$ for some $\sigma' \in \hat{\mathcal{G}}_{T'}$. Let τ be in $\hat{\mathcal{G}}_{T\sigma}$, and set $T^* = T'\sigma'$ $(\supset T\sigma)$. Then, $\tau = T\sigma|\tau^*$ for some $\tau^* \in \hat{\mathcal{G}}_{T^*}$. Evidently, $\sigma'\tau^*$ is in $\mathcal{G}(T', A; B)$ and $T|\sigma'\tau^* = \sigma(T\sigma|\tau^*) = \sigma\tau$. Hence, $\sigma\tau$ is in $\hat{\mathcal{G}}_T$.

Corollary 17.15. <u>Let</u> A <u>be left locally finite over</u> B. <u>If</u> $J(\mathcal{G}(T, A; B)) = B$ <u>for every</u> $T \in \mathcal{R}^{\circ}_{1.f}$ <u>then</u> $\hat{\mathcal{G}}$ <u>is a left q-system of</u> A/B.

<u>Proof</u>. Let T* be as in Lemma 17.14 (a). Then, $B = J(\mathcal{G}(T^*, A; B)) \cap T = J(T|\mathcal{G}(T^*, A; B)) = J(\hat{\mathcal{G}}_T)$. Now, our assertion is clear by Lemma 17.14 (b).

We shall consider here the following conditions:

(i) $J(\mathcal{G}(T, A; B)) = B$ for every $T \in \mathcal{R}^{\circ}_{1.f}$.

(ii) H/B is Galois and $B_2|\mathcal{G}(B_1, A; B) = \mathcal{G}(B_2, A; B)$ for every $B_1 \supset B_2$ in $\mathcal{R}_{1.f}$.

(iii) B is regular and $B_2|\mathcal{G}(B_1, A; B) = \mathcal{G}(B_2, A; B)$ for every $B_1 \supset B_2$ in $\mathcal{R}_{1.f}$.

(iv) A is B·V-A-irreducible.

(v) A is A-B·V-irreducible.

(vi) H/B is Galois and $[V_A^2(T):H]_L = [V:V_A(T)]_R$ for every $T \in \mathcal{R}^{\circ}_{1.f}$.

(vii) B and H are regular and $[V_A^2(T):H]_L = [V:V_A(T)]_R$ for every $T \in \mathfrak{L}^{\circ}_{l.f}$.

We state now the following principal theorem of this section.

Theorem 17.16. Let A be left locally finite over B.

(a) A/B is q-Galois if and only if any of the following equivalent conditions is satisfied: (Q1) (i) + (iv), (Q2) (i) + (v), (Q3) (i) + (vii), (Q4) (ii) + (iv), (Q5) (ii) + (v), and (Q6) (iii) + (vi).

(b) If A/B is q-Galois then A is locally finite and right q-Galois over B, $\mathfrak{G}$ is the unique left (and right) q-system of A/B, and A is inner Galois and locally finite over every simple intermediate ring A' of A/H left finite over H.

Proof. (a) If A/B is q-Galois then $\mathfrak{G}$ is a left q-system of A/B, H/B is outer Galois, and $B_2 | \mathfrak{G}(B_1, A; B) = \mathfrak{G}(B_2, A; B)$ for every $B_1 \supset B_2$ in $\mathfrak{L}_{l.f}$ (Lemmas 17.2 (a) and 17.8 and Th. 6.5 (a)). Next, if any of the conditions (Q1) - (Q3) is satisfied then $\hat{\mathfrak{G}}$ is a left q-system of A/B by Cor. 17.15. On the other hand, if any of the conditions (Q4) - (Q6) is satisfied then $\mathfrak{G}$ is a left q-system of A/B. In fact, $J(\mathfrak{G}(T, A; B)) = J(\mathfrak{G}(T, A; B)) \cap J(T|\tilde{V}) = J(T \cap H| \mathfrak{G}(T, A; B)) = J(\mathfrak{G}(T \cap H, A; B)) \subset J(T \cap H| \mathfrak{G}(H/B)) = B$. Our assertion is therefore an easy consequence of Prop. 7.11.

(b) By the validity of Prop. 17.11 (b), it remains to prove the last assertion. Obviously, $\tilde{V}$ induces a left q-system of A/H, and A is q-Galois and locally finite over H (Cor. 5.5 (d)). Hence, $\tilde{V}A_R$ is dense in $\mathrm{Hom}({}_HA, {}_HA)$, and then our assertion is a consequence of Cor. 6.10 (b).

Corollary 17.17. Let A be a division ring, and left locally finite over a division subring B. In order that A/B be q-Galois, it is necessary and sufficient that any of the following equivalent conditions be satisfied: (1) $J(\mathfrak{G}(T, A; B)) = B$ for every intermediate ring T of A/B left finite over B, (2) $B_2 | \mathfrak{G}(B_1, A; B) = \mathfrak{G}(B_2, A; B)$ for every intermediate rings $B_1 \supset B_2$ of A/B left finite over B

and $\mathcal{G}(T, A; B) \neq 1$ for every subring $T \supsetneqq B$ left finite over B, and (3) $B_2 | \mathcal{G}(B_1, A; B) = \mathcal{G}(B_2, A; B)$ for every intermediate rings $B_1 \supset B_2$ of A/B left finite over B and H/B is Galois.

Nagahara [8], [10], [11]; Nagahara-Tominaga [10], Nobusawa-Tominaga [2], Tominaga [12].

18. q-Galois extension

Let A be q-Galois and left locally finite over B. By Th. 17.16, H/B is outer Galois and A/H is locally finite. If B' is in $\mathcal{R}_{l.f}$ then it is f-regular and A/B' is q-Galois (Ths. 6.1 and 6.9). Since $V_A^2(B')$ is outer Galois over B', $B'[H]$ is a simple ring left finite over H (Th. 16.5 (a)). Accordingly, Th. 17.16 (b) yields $B'[H] = V_A^2(B')$. Moreover, as $H|\mathfrak{G}(V_A^2(B')/B') \subset \mathfrak{G}(H/B)$ (Ths. 6.5 (c) and 16.5 (a)), $\sigma \longrightarrow H|\sigma$ is a continuous monomorphism of the compact group $\mathfrak{G}(V_A^2(B')/B')$ into $\mathfrak{G}(H/B)$ and its image is a closed Galois group of $H/B' \cap H$ (Prop. 16.2 and Th. 16.5 (a)). Hence, $\sigma \longrightarrow H|\sigma$ is an isomorphism onto $\mathfrak{G}(H/B' \cap H)$ (Th. 16.5 (b)). Next, let A' be in $\mathcal{R}$. If $A'[H]$ is left finite over H then A' contains some $B' \in \mathcal{R}_{l.f}$ such that $A'[H] = B'[H]$, and so A' is f-regular. Conversely, if A' is f-regular then A' contains some $B' \in \mathcal{R}_{l.f}$ such that $V_A(B') = V_A(A')$. Hence, $A'[H] = B'[H] = V_A^2(B')$ is finite over H. Moreover, noting that $A'[H]$ is outer Galois and locally finite over A' (Th. 16.5), the above argument enables us to see that $\mathfrak{G}(A'[H]/A') \simeq \mathfrak{G}(H/A' \cap H)$ by the contraction map. In the sequel, those facts noted above will be used often without mention. Now, we shall prove the following transitivity theorem.

Theorem 18.1. *Assume that* A *is q-Galois and left locally finite over* B. *Let* A' *be in* $\mathcal{R}$, *and* H' *an intermediate ring of* H/B *that is Galois over* B.

(a) $A'[H']$ *is outer Galois and locally finite over* A' *and* $\mathfrak{G}(A'[H']/A') \simeq \mathfrak{G}(H'/A' \cap H')$ *by the contraction map*.

(b) *If* H^* *is an arbitrary subset of* H *then* $A'[H^*]$ *is in* $\mathcal{R}$ *and* $A'[H^*] \cap H = (A' \cap H)[H^*]$. *In particular, if* H^* *is an intermediate ring of* $H/A' \cap H$ *then* $A'[H^*] \cap H = H^*$.

(c) *If* A^* *is an intermediate ring of* $A'[H]/A'$ *then* $A'[A^* \cap H] = A^*$.

Proof. (b) and (c) are easy consequences of (a) and Th. 16.5. Thereby, it suffices to prove (a). We set $A' = \sum D'e'_{ij}$ where $E' = \{e'_{ij}\}$ is a system of matrix units with the division ring $D' = V_{A'}(E')$.

By Th. 6.3, A' contains a $B' \in \mathfrak{R}_{l.f}/E'$ such that $B'[F']$ is in $\mathfrak{R}_{l.f}$ for every finite subset F' of A', and so $A' = \cup B_\nu$, where B_ν runs over all the subrings of A' left finite over B'. Then, $A'[H] = \cup B_\nu[H]$ and every $A_\nu = B_\nu[H] = V_A^2(B_\nu)$ is a regular subring of A with $[A_\nu:H]_L < \infty$. Since the non-empty family $\{A_\nu\}$ is a directed set, $A'[H] = \cup A_\nu$ is in $\mathfrak{R}$ (Prop. 3.7). Next, $A'_\nu = A' \cap A_\nu$ is evidently simple and $V_A(A'_\nu) = V_A(B_\nu)$. Moreover, one will readily see that $A_\nu = A'_\nu[H]$, $A' = \cup A'_\nu$ and $A'_\nu \cap H = A' \cap H$. Hence, by the remark cited just before our theorem, $\mathfrak{G}(A_\nu/A') \simeq \mathfrak{G}(H/A'_\nu \cap H) = \mathfrak{G}(H/A' \cap H)$ by the contraction map. Accordingly, for every τ in $\mathfrak{G}(H/A' \cap H)$ there exists a uniquely determined $\tau_\nu \in \mathfrak{G}(A_\nu/A'_\nu)$ such that $H|\tau_\nu = \tau$, and then one will easily see that if $A_\mu \supset A_\nu$ then $A_\nu | \mathfrak{G}(A_\mu/A'_\mu) = A'_\nu[H] | \mathfrak{G}(A_\mu/A'_\mu) = \mathfrak{G}(A_\nu/A'_\nu)$. By the aid of this fact, we can consider the inverse limit $\mathfrak{H} = \varprojlim \mathfrak{G}(A_\nu/A'_\nu)$, which may be regarded as an automorphism group of $A'[H]$. Then, $A_\nu | \mathfrak{H} = \mathfrak{G}(A_\nu/A'_\nu)$ (Prop. 1.1), and so $A'[H]/A'$ is outer Galois. Further, $\mathfrak{H}$ is locally finite by the definition (Prop. 16.1 (a)). Hence, $A'[H]/A'$ is locally finite (Th. 16.1 (b)), and then it follows that $\mathfrak{H}$ is dense in $\mathfrak{G}(A'[H]/A')$ (Th. 16.5), whence it is easy to see that $H\mathfrak{G}(A'[H]/A') \subset H$. Consequently, by the usual argument, we see that $\mathfrak{G}(A'[H]/A') \simeq \mathfrak{G}(H/A' \cap H)$ by the contraction map. Now, assume that H' be an intermediate ring of H/B that is Galois over B. Then, $\mathfrak{G}(H'/B) = H' | \mathfrak{G}(H/B)$ by Th. 16.5 (a) and (d), and so by the validity of $H | \mathfrak{G}(A'[H]/A') = \mathfrak{G}(H/A' \cap H)$ we see that the simple ring $A'[H']$ is $\mathfrak{G}(A'[H]/A')$-invariant. Consequently, again by the usual argument, one will easily see our assertion.

Corollary 18.2. <u>Let A be q-Galois and left locally finite over B.</u>

(a) <u>If</u> B' <u>is in</u> $\mathfrak{R}_{l.f}$ <u>and</u> H^* <u>is an intermediate ring of</u> $H/B' \cap H$ <u>with</u> $[H^*:B]_L < \infty$, <u>then</u> $[B'[H^*]:B'] = [H^*:B' \cap H]$ <u>and</u> $[B'[H^*]:H^*]_L = [B':B' \cap H]_L$.

(b) <u>If</u> B' <u>is in</u> $\mathfrak{R}_{l.f}$ <u>and</u> H^* <u>is an intermediate ring of</u> $H/B' \cap H$, <u>then</u> $[B'[H^*]:H^*]_L \leqslant [B':B' \cap H]_L$. <u>Moreover, if</u> B' <u>is in</u> $\mathfrak{R}_{l.f}/\Delta$ <u>then</u> $B'[H^*] = H^* \cdot B'$ <u>and</u> $[B'[H^*]:H^*]_L = [A^*:A^* \cap H]_L =$

$[B':B'\cap H]_L$ *for every intermediate ring* H^* *of* $H/B'\cap H$ *and every intermediate ring* A^* *of* $B'[H]/B'$.

(c) *If* A' *is an f-regular intermediate ring of* A/B *then* A/A' *is locally finite*.

Proof. By Th. 18.1, H/B and $B'[H]/B'$ are outer Galois. We set $H' = B'\cap H$ and $\mathfrak{G}' = \mathfrak{G}(B'[H]/B')$.

(a) If M is an arbitrary $\mathfrak{G}(H/B)$-invariant shade of H^* then $\mathfrak{G}(B'[M]/B') = B'[M]\,|\,\mathfrak{G}' \simeq M\,|\,\mathfrak{G}' = \mathfrak{G}(M/H')$ (Ths. 7.4 and 18.1), which implies $[B'[M]:B'] = [M:H']$. Since $B'[H^*] \in \mathcal{R}_{l.f}$ and $H^* = B'[H^*]\cap H$ (Th. 18.1), the above argument yields $[B'[M]:B'[H^*]] = [M:H^*]$. Hence, we obtain $[B'[H^*]:B'] = [H^*:H']$, and consequently $[B'[H^*]:H^*]_L = [B':H']_L$.

(b) The first assertion is an easy consequence of (a). Now, assume that B' is in $\mathcal{R}_{l.f}/\Delta$. Since B' is linearly disjoint from H (Th. 18.1 and Lemma 17.9 (a)), we obtain $[B':B'\cap H]_L = [H^*\cdot B':H^*]_L \leqslant [B'[H^*]:H^*]_L \leqslant [B':B'\cap H]_L < \infty$, whence our assertion is obvious by Th. 18.1.

(c) A' contains some $B^* \in \mathcal{R}_{l.f}$ such that $V_A(A') = V_A(B^*)$. Then A is q-Galois and left locally finite over B^* and $V_A^2(B^*) \supset A' \supset B^*$ (Th. 6.9). Thereby, without loss of generality, we may assume that A' is contained in H. Let F be an arbitrary finite subset of A. Choose an arbitrary B' in $\mathcal{R}_{l.f}/F$, and set $H^* = A'[B'\cap H]$. Then, $[H^*:A'] < \infty$ by Th. 16.5 (a). Moreover, by (b), $[B'[H^*]:H^*]_L \leqslant [B':B'\cap H]_L < \infty$. Hence, it follows $[B'[H^*]:A']_L < \infty$, which means the left local finiteness of A/A'. Recalling that A/B is right locally finite and right q-Galois (Th. 17.16), we see that A/A' is right locally finite, too.

Proposition 18.3. *Let* A/B *be q-Galois and left locally finite. If* B' *is in* $\mathcal{R}_{l.f}$ *and* σ *in* $\mathfrak{G}(B', A; B)$ *then* $\infty > [B':B] \geqslant [V:V_A(B')] = [V:V_A(B'\sigma)] = [V_A^2(B'):H] = [B':B'\cap H]$.

Proof. If we set $H^* = (B'\cap H)[\Delta]$ and $B^* = B'[H^*]$, then $H^* = B^*\cap H$ (Th. 18.1), and then $[V_A^2(B'):H]_L = [B'[H]:H]_L = [B^*[H]:H]_L =$

$[B^*:B^* \cap H]_L = [B'[H^*]:H^*]_L = [B':B' \cap H]_L$ (Cor. 18.2 (b), (a)). Since A is $B' \cdot V_A(B')$-A-irreducible and A-$B\cdot V$-irreducible (Ths. 6.9 and 17.16), it follows $[B':B' \cap H]_L \geqslant [V:V_A(B')]_R \geqslant [V_A^2(B'):H]_L = [B':B' \cap H]_L$ (Prop. 5.4). Hence, we obtain $[B':B' \cap H]_L = [V:V_A(B')]_R = [V_A^2(B'):H]_L$, and similarly $[B':B' \cap H]_R = [V:V_A(B')]_L = [V_A^2(B'):H]_R$. Since $[B' \cap H:B]_L = [B' \cap H:B]_R$ by Th. 16.5 (c), it is only left to prove $[B':B' \cap H]_L = [B':B' \cap H]_R$ and $[V:V_A(B'\sigma)] = [V:V_A(B')]$. Noting that A is $B' \cdot V_A(B')$-A-irreducible, we have $[B':B' \cap H]_L \geqslant [V:V_A(B')]_L$ (Prop. 5.4 (b)). Symmetrically, we obtain $[B':B' \cap H]_R \geqslant [V:V_A(B')]_R$. Hence, it follows $[B':B' \cap H]_L = [V:V_A(B')]_R \leqslant [B':B' \cap H]_R = [V:V_A(B')]_L \leqslant [B':B' \cap H]_L$, namely, $[B':B' \cap H]_L = [B':B' \cap H]_R$. Finally, by Th. 6.5 (c), there holds $B'\sigma \cap H = (B' \cap H)\sigma$. Then, we obtain $[V:V_A(B'\sigma)] = [B'\sigma:B'\sigma \cap H] = [B'\sigma:(B' \cap H)\sigma] = [B':B' \cap H] = [V:V_A(B')]$.

Corollary 18.4. _Let_ A _be q-Galois and left locally finite over_ B.

(a) _If_ $A' \in \mathcal{R}$ _is f-regular then_ $\infty > [V:V_A(A')] = [V_A^2(A'):H] = [A':A' \cap H]$.

(b) _If_ $A' \in \mathcal{R}$ _is f-regular then_ $A' | \mathcal{G}(A^*, A; B) \subset \mathcal{G}(A', A; B)$ _for every_ $A^* \in \mathcal{R}/A'$. _In particular_, $H | \mathcal{G}(A^*, A; B) \subset \mathcal{G}(H, A; B) = \mathcal{G}(H/B)$ _for every_ $A^* \in \mathcal{R}/H$.

(c) _If_ A' _is an intermediate ring of_ A/B _such that_ A _is_ A'-A-_irreducible and_ $[V:V_A(A')]_R < \infty$ _(or_ $[V:V_A(A')]_L < \infty$ _) then_ A' _is f-regular_. _Conversely, if_ A' _is f-regular and_ $V_A(A')$ _is a division ring then_ A _is_ A'-A-_irreducible_.

Proof. (a) Let N be an arbitrary $\mathcal{G}(H/B)$-invariant shade of Δ. Then, by Th. 18.1, we have $[A'[N]:A'] = [N:A' \cap N] < \infty$ and $A'[N] \cap H = A'[(A' \cap H)[N]] \cap H = (A' \cap H)[N]$. Since $A' \cap H$ is in $\mathcal{R}$ (Th. 16.5), we obtain $[A'[N] \cap H:A' \cap H] = [(A' \cap H)[N]:A' \cap H] = [N:A' \cap N] = [A'[N]:A'] < \infty$ again by Th. 18.1. We choose here a simple intermediate ring B' of A/B such that $[B':B]_L < \infty$ and $V_A(B') = V_A(A')$, and set $B^* = B'[N]$. Then, B^* is in $\mathcal{R}_{l.f}$ (Th. 18.1). Recalling that

$B^*[H] = V_A^2(B^*) \supset A'[N] \supset B^* \supset \Delta$, Cor. 18.2 and Prop. 18.3 imply that $[A'[N]:A'[N] \cap H]_L = [B^*:B^* \cap H] = [V:V_A(B^*)] = [V:V_A(B')] < \infty$. Combining this with $[A'[N] \cap H:A' \cap H] = [A'[N]:A'] < \infty$, it follows at once $[A':A' \cap H]_L = [A'[N]:A'[N] \cap H]_L = [V:V_A(B')] = [V:V_A(A')]$. Then, we obtain symmetrically $[A':A' \cap H]_R = [V:V_A(B')] = [V_A^2(B'):H] = [V_A^2(A'):H]$ by Th. 17.16 and Prop. 18.3.

(b) By (a), there exists some $B' \in \mathcal{R}_{l.f}$ such that $A' = B'[A' \cap H]$. If σ is in $\mathcal{G}(A^*, A; B)$ then $B'\sigma \in \mathcal{R}_{l.f}$ and $(A' \cap H)\sigma \subset (A^* \cap H)\sigma \subset H$ (Th. 6.5 (b) and (c)). Hence, $A'\sigma = (B'\sigma)[(A' \cap H)\sigma]$ is in $\mathcal{R}$ (Th. 18.1). The latter is now evident by Th. 16.5 (a).

(c) Since A is A'-A-irreducible, $V_A(A')$ is a division ring and $V_A^2(A')$ is in $\mathcal{R}$ (Prop. 5.4 (a)). Since A is A-$B\cdot V$-irreducible (Th. 17.16) and $A'[H]$-A-irreducible, we have $[A'[H]:H]_L \leqslant [V_A^2(A'):H]_L \leqslant [V:V_A(A')]_R = [V:V_A(A'[H])]_R \leqslant [A'[H]:H]_L$ (Prop. 5.4 (b)), whence it follows that $A'[H]$ coincides with the f-regular intermediate ring $V_A^2(A')$. Hence, we can find a finite subset F of H and an intermediate ring B' of A'/B such that $V_A(B'[F]) = V_A(A')$ and $B'[F] \in \mathcal{R}_{l.f}$. We shall prove now that A is B'-A-irreducible. Let a be a non-zero element of A. Since $B'aA$ is a B-A-submodule of the B-A-completely reducible module A (Th. 17.16 and Prop. 5.4), $B'aA = vA$ with some $v \in V$. Then, we see that $B'aA = vA$ is left $B'[F]$-admissible. Recalling that A is $B'[F]$-A-irreducible (Th. 6.1), it follows then $B'aA = A$. Hence, B' and A' are simple by Prop. 3.8. (If $[V:V_A(A')]_L < \infty$ then there exists some $B^* \in \mathcal{R}^{\circ}_{l.f}$ such that $V_A(B^*) \subset V_A(A')$, and then $[V:V_A(A')]_R \leqslant [V:V_A(B^*)]_R < \infty$ by Prop. 5.4.) The converse part is evident by Th. 6.1 (b).

As an application of Prop. 18.3, we shall present the following interesting theorem.

Theorem 18.5. _Let_ A _be_ $B\cdot V$-A-_irreducible and_ A-$B\cdot V$-_irreducible, and_ $\mathfrak{H}$ _a Galois semigroup of_ A/B.

(a) *Let* T *be a* B-B-*submodule of* A *(possessing a left* B-*basis and a right* B-*basis). If* A/H *is left locally finite then* $[T:B]_L = [T:B]_R$, *provided we do not distinguish between two infinite dimensions.*

(b) *Let* V *be contained in* B. *If* T *is an intermediate ring of* A/B *then* $[T:B]_L = [T:B]_R$, *provided we do not distinguish between two infinite dimensions.*

Proof. One may remark first that B and H are regular by Prop. 5.4 and Cor. 5.6, and assume that $\mathfrak{h}$ contains $\tilde{V}$.

(a) Since A is $H \cdot V$-A-irreducible and left locally finite over $H = V_A^2(H)$, A/H is locally finite (Cor. 17.12). Hence, by the symmetry of our assumption, it suffices to prove that if $[T:B]_L < \infty$ then $[T:B]_R \leqslant [T:B]_L$. Now, let $\{\varepsilon_1, \dots, \varepsilon_t\}$ be a V_R-basis of $(T|\mathfrak{h})V_R$ that forms at the same time an A_R-basis of $(T|\mathfrak{h})A_R$ (Lemma 5.8). By Prop. 18.3, there holds then $\infty > [H[E, \cup_1^t T\varepsilon_i]:H] = [V:V_A(H[E, \cup_1^t T\varepsilon_i])]$. Hence, $[T:B]_R \leqslant [T:B]_L$ (Prop. 5.9).

(b) Again by the symmetry of our assumption, it suffices to prove that if $[T:B]_L < \infty$ then $[T:B]_R \leqslant [T:B]_L$. Since $U' = V_A(T) = V_B(T) \subset V_A(T\mathrm{Hom}({}_BT, {}_BA)) \subset V$ (field) and $[V:U'] \leqslant [T:B]_L < \infty$ (Prop. 5.4), our assertion is again a consequence of Prop. 5.9.

As a direct consequence of Th. 18.5 (a), we obtain the following:

Corollary 18.6. *Let* A *be* $B \cdot V$-A-*irreducible and* A-$B \cdot V$-*irreducible, and* T *an intermediate ring of* A/B. *If* $J(\mathfrak{G}) = B$ *and* A/H *is left locally finite then* $[T:B]_L = [T:B]_R$, *provided we do not distinguish between two infinite dimensions.*

Lemma 18.7. *Let* A *be q-Galois and left locally finite over* B. *If* B' *is in* $\mathcal{R}_{l.f}$ *then* $B' | \mathfrak{G}(V_A^2(B'), A; B) = \mathfrak{G}(B', A; B)$.

Proof. By Th. 18.1, $H^* = V_A^2(B') = B'[H]$ is outer Galois over B'. We set here $H^* = \cup B'_\alpha$, where B'_α ranges over all the $\mathfrak{G}(H^*/B')$-invariant shades. Now, let ρ be in $\mathfrak{G}(B', A; B)$. Then the set $\mathfrak{E}_\alpha = \{\rho' \in \mathfrak{G}(B'_\alpha, A; B);\ B'|\rho' = \rho\}$ is non-empty by Th. 6.5. If ρ' is in $\mathfrak{E}_\alpha$, then $B'_\alpha\rho'/B'\rho$ is Galois and $B'_\alpha\rho' = ((B'_\alpha \cap H)[B'])\rho' \subset$

$H[B'\rho] = V_A^2(B'\rho)$ (Th. 18.1). Hence, $\mathcal{G}(B'_\alpha\rho'/B'\rho) = B'_\alpha\rho'|\mathcal{G}(V_A^2(B'\rho)/B'\rho)$ $= \mathcal{G}(B'_\alpha\rho', A; B'\rho)$ (Ths. 6.5 and 16.5 (b) and (d)). Consequently, $\mathcal{G}(B'_\alpha\rho', A; B'\rho) \simeq \mathcal{G}(B'_\alpha/B')$ is finite, and so $\mathcal{E}_\alpha$ is finite, too. Thus, by Th. 6.5 and Prop. 1.1, the inverse limit $\mathcal{E} = \varprojlim \mathcal{E}_\alpha$ is non-empty, which means that ρ can be extended to an isomorphism ρ^* of H^* into A. Since $V_A(H^*\rho^*) = V_A(\cup((H \cap B'_\alpha)[B'])\rho^*) = V_A(B'\rho)$, ρ^* is in $\mathcal{G}(H^*, A; B)$, and so $\mathcal{G}(B', A; B) \subset B'|\mathcal{G}(H^*, A; B)$. The converse inclusion is secured by Th. 6.5.

Theorem 18.8. _Let_ A _be q-Galois and left locally finite over_ B.

(a) _If_ $A_1 \supset A_2$ _are f-regular intermediate rings of_ A/B _then_ $\mathcal{G}(A_2, A; B) = A_2|\mathcal{G}(A_1, A; B)$. _In particular, if_ A_1 _is an f-regular intermediate ring of_ A/H _then_ $A_1 = V_A^2(A_1)$, $[A_1:H] < \infty$ _and_ $H|\mathcal{G}(A_1, A; B) = \mathcal{G}(H/B)$.

(b) _If_ $A_1 \supset A_2$ _are f-regular intermediate rings of_ A/B _then_ $J(\mathcal{G}(A_1, A; A_2)) = A_2$.

(c) _If_ A' _is an f-regular intermediate ring of_ A/B _then_ A _is q-Galois and locally finite over_ A'.

(d) _If_ A' _is an f-regular intermediate ring of_ A/B _then_ $[V:V_A(A'\sigma)] = [V:V_A(A')]$ _and_ $|V_A(A'\sigma)| = |V_A(A')|$ _for every_ $\sigma \in \mathcal{G}(A', A; B)$.

Proof. (a) Obviously, A_2 contains $B_2 \in \mathfrak{L}_{1.f}$ such that $V_A(B_2) = V_A(A_2)$. Then, $A'_2 = V_A^2(A_2) = V_A^2(B_2) = B_2[H]$ is finite over H (Prop. 18.3). We shall prove first $\mathcal{G}(A_2, A; B) \subset A_2|\mathcal{G}(A'_2, A; B)$. If σ is in $\mathcal{G}(A_2, A; B)$ then $B_2|\sigma = B_2|\tau$ for some $\tau \in \mathcal{G}(A'_2, A; B)$ (Cor. 18.4 and Lemma 18.7). Recalling that $A_2 = B_2[A_2 \cap H]$ (Th. 18.1), we see that $A_2\sigma = (B_2\sigma)[(A_2 \cap H)\sigma] \subset (B_2\tau)[H] = A'_2\tau$ (Cor. 18.4 (b)), and so $\sigma\tau^{-1}$ is contained in $A_2|\mathcal{G}(A'_2/B_2)$ (Ths. 18.1 and 16.5 (a)), whence it follows $\sigma \in A_2|\mathcal{G}(A'_2, A; B)$. We have seen thus $\mathcal{G}(A_2, A; B)$ $= A_2|\mathcal{G}(A'_2, A; B)$ (Cor. 18.4 (b)). Similarly, if $A'_1 = V_A^2(A_1)$ then $\mathcal{G}(A_1, A; B) = A_1|\mathcal{G}(A'_1, A; B)$. Next, we shall prove $A'_2|\mathcal{G}(A'_1, A; B) =$

$\mathcal{G}(A_2', A; B)$. Between A_1' and B_2 there exists some $B_1' \in \mathcal{R}_{1.f}$ such that $A_1' = V_A^2(B_1') = B_1'[H]$. If $B_2' = A_2' \cap B_1'$ then $B_2 < B_2' < A_2' = V_A^2(B_2)$, and hence B_2' is in $\mathcal{R}_{1.f}$ (Ths. 18.1 and 16.5 (a)) and $A_2' = V_A^2(B_2') = B_2'[H]$. Since $B_2'|\mathcal{G}(A_2', A; B) = \mathcal{G}(B_2', A; B) = B_2'|\mathcal{G}(B_1', A; B) = B_2'|\mathcal{G}(A_1', A; B)$ (Th. 6.5 and Lemma 18.7), for every $\tau' \in \mathcal{G}(A_2', A; B)$ we can find some $\rho' \in \mathcal{G}(A_1', A; B)$ such that $B_2'|\rho' = B_2'|\tau'$. As A/B_2' is q-Galois (Th. 6.9) and $A_2'\tau' = (B_2'\tau')[H] = (B_2'\rho')[H] = A_2'\rho'$ (Cor. 18.4 (b)), $\tau'\rho'^{-1}$ is in $\mathcal{G}(A_2'/B_2') = \mathcal{G}(A_2'/A_2' \cap B_1') = A_2'|\mathcal{G}(A_1'/B_1')$ (Th. 18.1). Hence, τ' is in $A_2'|\mathcal{G}(A_1', A; B)$, namely, $\mathcal{G}(A_2', A; B) = A_2'|\mathcal{G}(A_1', A; B)$ (Cor. 18.4 (b)). It follows therefore $\mathcal{G}(A_2, A; B) = A_2|\mathcal{G}(A_2', A; B) = A_2|(A_2'|\mathcal{G}(A_1', A; B)) = A_2|(A_1|\mathcal{G}(A_1', A; B)) = A_2|\mathcal{G}(A_1, A; B)$. The latter is obvious by Cor. 18.4 (a) and (b).

(b) By Th. 6.9 (a), we may assume that A_2 is contained in H. Then, noting that $\mathcal{G}(A_1, A; A_2) \supset A_1|\tilde{V}$, we obtain $J(\mathcal{G}(A_1, A; A_2)) = J(\mathcal{G}(A_1, A; A_2)) \cap H = J(\mathcal{G}(A_1 \cap H, A; A_2)) = J(A_1 \cap H|\mathcal{G}(H/A_2)) = A_2$ ((a) and Ths. 6.5 (c) and 16.5).

(c) Again by Th. 6.9 (a), we may assume that A' is contained in H (and so $V = V_A(A')$). Then, A is $A' \cdot V_A(A')$-A-irreducible (Th. 17.16) and locally finite over A' (Cor. 18.2 (c)). Now, let $\mathcal{R}^*$ be the set of all $T \in \mathcal{R}^\circ/A'$ such that $[T:A']_L < \infty$. Then $\mathcal{J}' = \{\mathcal{G}(T, A; A'); T \in \mathcal{R}^*\}$ is a left q-system of A/A' by (a) and (b). Hence, Th. 17.16 yields at once our assertion.

(d) Choose a simple intermediate ring B' of A'/B such that $V_A(B') = V_A(A')$. Since $V_A^2(B') = B'[H] = A'[H]$ is f-regular, by (a) we can find $\sigma' \in \mathcal{G}(A'[H], A; B)$ such that $\sigma = A'|\sigma'$. Then, by Cor. 18.4 (b) and Prop. 18.3, we obtain $[V:V_A(A')] = [V:V_A(B')] = [V:V_A(B'\sigma)] = [V:V_A(B'[H]\sigma')] = [V:V_A(A'\sigma)]$. In particular, the last implies $V_A(A'\sigma) = V_A(B'\sigma)$, and hence the latter assertion is obvious by Th. 6.5 (b).

Now, we shall consider the following condition (viii) besides

(i) - (vii) introduced in §17.

(viii) H/B is Galois and $H|\mathfrak{G}(A', A; B) \supset \mathfrak{G}(H/B)$ for every $A' \in \mathcal{R}^{o}/H$ with $[A':H]_L < \infty$.

Then, we can add other equivalent conditions to Th. 17.16 (a).

Corollary 18.9. Let A be left locally finite over a simple subring B. In order that A/B be q-Galois, it is necessary and sufficient that any of the following equivalent conditions be satisfied: (Q7) (iv) + (viii) and (Q8) (v) + (viii).

Proof. If A/B is q-Galois then all the conditions (i) - (viii) are satisfied (Ths. 17.16 and 18.8). Conversely, assume (Q7) or (Q8). Then, A/H is left locally finite by Cor. 5.5 (d). If T is in $\mathcal{R}^{o}_{l.f}$ then $J(\mathfrak{G}(T, A; B)) \subset J(T|\mathfrak{G}(T[H], A; B)) = J(T \cap H|\mathfrak{G}(T[H], A; B)) \subset J(T \cap H|\mathfrak{G}(H/B)) = B$. Hence, A/B is q-Galois by Th. 17.16.

Let A be q-Galois over B. A (*)-regular subgroup $\mathfrak{H}$ of $\mathfrak{G}$ is called a $(*_f)$-regular subgroup of $\mathfrak{G}$ if $[V:V(\mathfrak{H})]_R < \infty$, and a $(*_f)$-regular subgroup $\mathfrak{H}$ of $\mathfrak{G}$ with simple $J(\mathfrak{H})$ is called an f-regular subgroup of $\mathfrak{G}$. If A/B is q-Galois and left locally finite, then every $(*_f)$-regular subgroup of $\mathfrak{G}$ is proved to be f-regular. To see this, the following lemma will be needed.

Lemma 18.10. Let A be q-Galois and left locally finite over B, and $\mathfrak{G}'$ a $(*_f)$-regular subgroup of $\mathfrak{G}$. If $A' = J(\mathfrak{G}')$ then $[A':A' \cap H]_L < \infty$.

Proof. Let N be a $\mathfrak{G}(H/B)$-invariant shade of Δ, $\mathfrak{G}^* = \mathfrak{G}(N) \cap \mathfrak{G}' = \mathfrak{G}'(N)$, $A^* = J(\mathfrak{G}^*)$ $(\supset A'[N])$ and $H^* = A^* \cap H$. Then, $\mathfrak{G}^*$ is an invariant subgroup of $\mathfrak{G}'$ and $(\mathfrak{G}':\mathfrak{G}^*) = \#(N|\mathfrak{G}') \leq \#\mathfrak{G}(N/B) = [N:B] < \infty$ (Th. 7.4). As $H^* = A^* \cap H$ is a $\mathfrak{G}'$-invariant simple subring of H (Th. 16.5 (a)), $H^*/A' \cap H$ is outer Galois and $[H^*:A' \cap H] = \#(H^*|\mathfrak{G}') \leq (\mathfrak{G}':\mathfrak{G}^*) < \infty$ (Th. 7.4). Further, we can see that $V(\mathfrak{G}^*) = V(\mathfrak{G}') = V_A(B[F])$ for some finite subset F of A. Now, let B_o be in $\mathcal{R}_{l.f}/B[F]$. Then $V(\mathfrak{G}^*) = V_A(B[F]) \supset V_A(B_o)$ yields $A^*[H] \subset V_A(V(\mathfrak{G}^*)) \subset V_A^2(B_o)$, so that $[A^*[H]:H] \leq [V_A^2(B_o):H] < \infty$

by Prop. 18.3. Noting that $[A^*:H^*]_L = [H\cdot A^*:H]_L$ (Lemma 17.9 (a)), we obtain $[A':A'\cap H]_L \leq [A^*:H^*]_L\cdot[H^*:A'\cap H] = [H\cdot A^*:H]_L\cdot[H^*:A'\cap H]$ $\leq [V_A^2(B_o):H]\cdot[H^*:A'\cap H] < \infty$.

Lemma 18.11. *Let A be q-Galois and left locally finite over B, and V' a simple subring of V such that $[V:V']_R < \infty$. If $V_A(V_A(V')[F]) \subset V'$ for some finite subset F of A then $V_A(V')$ is a simple ring.*

Proof. By Cor. 17.12 and Th. 17.16, A/H is h-Galois and locally finite. Hence, we may assume that A is h-Galois and locally finite over B and $H = B$. As $V_A(K) = \sum Vd_{hk}$ (simple), $V_A^2(K) = K$ and $B\cdot V = K\cdot\sum Vd_{hk}$, by the light of Cor. 17.12, we may assume further that B is a division ring. Accordingly, A is then V-A-irreducible (Cor. 17.12 and Prop. 5.4). We set $B' = V_A(V')$. Since A is A-$B\cdot V$-irreducible (Cor. 17.12), there holds $[B':B] \leq [V:V']_R < \infty$ (Prop. 5.4). If B'' is in $\mathfrak{L}^{o}_{l.f}/B'[F]$ and $V'' = V_A(B'')$ ($\subset V'$) then $V_A(V'') = B''$ (Th. 17.18 (b)) and $\infty > [B'':B] = [V:V''] = [V:V_A^2(V'')\cap V]$ (Prop. 18.3). Since A is V-A-irreducible, Prop. 16.7 (b) yields then $\mathrm{Hom}({}_{V''}V, {}_{V''}A) = (V|\widetilde{B''})A_R = \oplus_1^t (V|\sigma_i)A_R$ ($\sigma_i \in \widetilde{B''}$), where every $(V|\sigma_i)A_R$ is V_R-A_R-irreducible and every $V|\sigma_i$ is free over A_R (Prop. 5.7 (a)). Hence, the V_R-A_R-submodule $\mathrm{Hom}({}_{V'}V, {}_{V'}A)$ of $\mathrm{Hom}({}_{V''}V, {}_{V''}A)$ is completely reducible: $\mathrm{Hom}({}_{V'}V, {}_{V'}A) = \oplus_1^s \mathfrak{m}_j$ with V_R-A_R-irreducible submodules $\mathfrak{m}_j$'s. By Prop. 5.7 (c), every $\mathfrak{m}_j$ is of the form $(V \mid \sigma u_L)A_R$ with some σ in $\{\sigma_i\}$ and non-zero u, and so we may set $\mathfrak{m}_j = (V|b_{jL})A_R$ with some b_j. Noting that $V|b_{jL}$ is contained in $\mathrm{Hom}({}_{V'}V, {}_{V'}A)$, it is obvious that b_j is in B'. Now, let $M = V'vA$ ($v \in V$) be a V'-A-submodule of A such that $[M|A_R]$ is minimal among the non-zero V'-A-submodules of A of the form $V'xA$ ($x \in V$). If $V'yA$ is an arbitrary V'-A-irreducible submodule of M then $BV'yA = V'(ByA) = V'(u'A)$ with some $u' \in V$, for ByA is a direct summand of the completely reducible B-A-module A (Th. 6.1 (b)).

Hence, by the minimality of $[M|A_R]$, we obtain $M = V'(u'A) = \sum_{b\in B} V'byA = \oplus_1^q V'y_iA$, where $V'y_iA$ is V'-A-isomorphic to $V'yA$. Since $V'v \subset V$ and A is $V'_L\cdot V_{\mathfrak{A}}(V'_L)$-irreducible, it follows then $V = v(V'_L\cdot V\ (V'_L)) = (V'v)\mathrm{Hom}({}_{V'}V,\ {}_{V'}A) = \sum V'v\,\mathfrak{m}_j = \sum_{i,j} b_j(V'y_iA)$. Now, b_j being contained in B', every $b_j(V'y_iA)$ is V'-A-homomorphic to $V'y_iA \simeq V'yA$. Hence, A is homogeneously V'-A-completely reducible, and consequently B' is a simple ring.

Theorem 18.12. Let A be q-Galois and left locally finite over B, and $\mathfrak{G}'$ a $(*_f)$-regular subgroup of $\mathfrak{G}$ with $A' = J(\mathfrak{G}')$.

(a) $\mathfrak{G}'$ is f-regular and dense in $\mathfrak{G}(A')$, and A is h-Galois and locally finite over A'.

(b) $\tilde{V}\cdot\mathrm{Cl}\ \mathfrak{G}' = \mathfrak{G}(A'\cap H)$.

(c) If $\mathfrak{H}$ is an open subgroup of $\mathfrak{G}$ then the group index $(\mathrm{Cl}\,\mathfrak{G}' : (\mathfrak{H}\cap \mathrm{Cl}\,\mathfrak{G}')\cdot V(\mathfrak{G}')^{\sim})$ is finite.

Proof. One may remark here that $H' = A'\cap H$ is f-regular (Ths. 17.16 and 16.5). As $[V:V(\mathfrak{G}')]_R < \infty$ and $V(\mathfrak{G}') = V_A^2(V(\mathfrak{G}'))$, $V_A^2(A') = V_A(V(\mathfrak{G}'))$ is simple by Lemma 18.11. Further, by Lemma 18.10, there holds $[A':H']_L < \infty$. Since A/H' is locally finite (Th. 18.8 (c)), the centralizer of A' in $V_A^2(A')$ coincides with the center of $V_A^2(A')$ and $J(V_A^2(A')|\mathfrak{G}') = A'$, Cor. 7.5 proves that A' is simple, and so A/A' is q-Galois and locally finite (Th. 18.8 (c)). If T is in $\mathfrak{L}^\circ/A'$ and $[T:A']_L < \infty$ then A is T-A-irreducible and $\infty > [T:T\cap V_A^2(A')] = [V_A(A'):V_A(T)]$ (Prop. 18.3). Hence, A/A' is h-Galois and $\mathfrak{G}'$ is dense in $\mathfrak{G}(A')$ (Prop. 16.7 (b)), which completes the proof of (a). Recalling here that $[T:H']_L = [T:A']_L\cdot[A':H']_L < \infty$, for every σ in $\mathrm{Cl}(\tilde{V}\cdot\mathrm{Cl}\ \mathfrak{G}')$ we can find an element $\tau \in \tilde{V}\cdot\mathrm{Cl}\ \mathfrak{G}'$ such that $T|\tau = T|\sigma$, and then $\sigma\tau^{-1}$ is contained in $\mathfrak{G}(T) \subset \mathfrak{G}(A') = \mathrm{Cl}\ \mathfrak{G}'$ by (a). Hence, σ is contained in $\tilde{V}\cdot\mathrm{Cl}\ \mathfrak{G}'$, which means that $\tilde{V}\cdot\mathrm{Cl}\ \mathfrak{G}'$ is a closed $(*_f)$-regular subgroup of $\mathfrak{G}$ with $J(\tilde{V}\cdot\mathrm{Cl}\ \mathfrak{G}') = H'$. Accordingly, (b) is a consequence of (a). Finally, we shall prove (c). Since $J(\mathrm{Cl}\,\mathfrak{G}') = A'$ and $V(\mathrm{Cl}\,\mathfrak{G}') = V(\mathfrak{G}')$, it suffices to prove our assertion for closed $\mathfrak{G}' = \mathfrak{G}(A')$. Moreover, without loss of generality, we may assume that $\mathfrak{H} = \mathfrak{G}(B')$ for some $B' \in \mathcal{R}^{o}_{1.f}$. If $T = A'[B']$ then $[T:A']_L < \infty$ and $\mathfrak{G}'(T)$ is a closed $(*_f)$-regular subgroup of $\mathfrak{G}'$ with $J(\mathfrak{G}'(T)) = T$ (Cor. 6.10), and then it follows $(\mathfrak{H} \cap \mathfrak{G}')\cdot V(\mathfrak{G}')^{\sim} = \mathfrak{G}'(T)\cdot V_A(A')^{\sim} = \mathfrak{G}'(T \cap V_A^2(A'))$ by (b). Hence, we obtain $(\mathfrak{G}':(\mathfrak{H} \cap \mathfrak{G}')\cdot V(\mathfrak{G}')^{\sim}) = (\mathfrak{G}':\mathfrak{G}'(T \cap V_A^2(A'))) = \#(T \cap V_A^2(A') \mid \mathfrak{G}') = [T \cap V_A^2(A'):A'] < \infty$ (Th. 16.5 (c)).

We shall conclude this section with the following theorem, that will be needed alter to expose the gap between (*)-regularity and N*-regularity.

Theorem 18.13. <u>Let</u> A <u>be q-Galois and left locally finite over</u> B, <u>and</u> $\mathfrak{G}'$ <u>an N*-regular subgroup of</u> $\mathfrak{G}$. <u>Then,</u> $\mathfrak{G}'$ <u>is</u> $(*_f)$-<u>regular if and only if</u> $[V:I(\mathfrak{G}')]_R < \infty$, $V_A^2(I(\mathfrak{G}')) = I(\mathfrak{G}') = I(\mathrm{Cl}\,\mathfrak{G}')$ <u>and</u> $(\mathrm{Cl}\,\mathfrak{G}':(\mathfrak{H} \cap \mathrm{Cl}\,\mathfrak{G}')\cdot I(\mathfrak{G}')^{\sim}) < \infty$ <u>for every open subgroup</u> $\mathfrak{H}$ <u>of</u> $\mathfrak{G}$.

<u>Proof</u>. If $\mathfrak{G}'$ is $(*_f)$-regular then $I(\mathfrak{G}')$ coincides with $V(\mathfrak{G}')$, and hence the only if part is obvious by Th. 18.12. To prove the if part, we may restrict our proof to the case that $\mathfrak{G}'$ is closed. By Th. 18.12 (a), $V_A(I(\mathfrak{G}'))$ is simple and there exists a finite subset F of $V_A(I(\mathfrak{G}'))$ such that $V_A(B[F]) = I(\mathfrak{G}')$. If we set $\mathfrak{H} = \mathfrak{G}(B[F])$ then $\mathfrak{G}^* = \mathfrak{H} \cap \mathfrak{G}'$ is a subgroup of $\mathfrak{H}$ containing $I(\mathfrak{G}')^{\sim}$, and so there holds $B[F] \subset J(\mathfrak{G}^*) \subset V_A(I(\mathfrak{G}'))$, which implies $I(\mathfrak{G}') = V_A(B[F]) \supset V(\mathfrak{G}^*) \supset V_A^2(I(\mathfrak{G}')) = I(\mathfrak{G}')$. We see therefore that $\mathfrak{G}^*$ is a closed $(*_f)$-regular subgroup of $\mathfrak{G}$ with $V(\mathfrak{G}^*) = I(\mathfrak{G}')$. By assumption, $(\mathfrak{G}':\mathfrak{G}^*) < \infty$: $\mathfrak{G}' = \cup_1^m \mathfrak{G}^*\sigma_i$. Now, we set $A^* = J(\mathfrak{G}^*)$ and $A' = J(\mathfrak{G}')$. Then, $\mathfrak{G}^* = \mathfrak{G}(A^*)$ and A is h-Galois and locally finite over A^* (Th. 18.12 (a)), and hence $A^{**} = A^*[\cup_1^m A^*\sigma_i]$ is a $\mathfrak{G}'$-invariant simple ring as an intermediate ring between $V_A^2(A^*) = V_A(V(\mathfrak{G}^*)) = V_A(I(\mathfrak{G}'))$ and A^* (Ths. 17.16 and 16.5). Let σ be an arbitrary element of $\mathfrak{G}'$. If σ induces an inner automorphism in A^{**}:

$A^{**}|\sigma = A^{**}|\tilde{v}$ ($v \in V_{A^{**}}(A')$), then $A^* \cap H|\sigma = 1$, and so σ is contained in $\mathfrak{G}(A^* \cap H) = \mathfrak{G}^*\cdot\tilde{V}$ (Th. 18.12 (b)): $\sigma = \tau\tilde{u}$ ($\tau \in \mathfrak{G}^*$, $u \in V$). But then, $\tau^{-1}\sigma = \tilde{u} \in \mathfrak{G}' \cap \tilde{V} = I(\mathfrak{G}')$ implies $\sigma \in \tau\cdot I(\mathfrak{G}')^{\sim} \subset \mathfrak{G}^*$, so that v is contained in $V_{A^{**}}(A^*) = V_{A^{**}}(A^{**})$. Hence, $A^{**}|\sigma = A^{**}|\tilde{v} = 1$, which means that $A^{**}|\mathfrak{G}'$ is an outer group of finite order. Accordingly, A^{**} is outer Galois and finite over the simple ring A' (Th. 7.4). Moreover, noting that $\mathfrak{G}^* = \mathfrak{G}^*\cdot(\tilde{V} \cap \mathfrak{G}')$ $= \mathfrak{G}^*\cdot\tilde{V} \cap \mathfrak{G}' = \mathfrak{G}(A^* \cap H) \cap \mathfrak{G}' = \mathfrak{G}'(A^* \cap H)$, we obtain $[A^*:A'] = \#(A^*|\mathfrak{G}') = (\mathfrak{G}':\mathfrak{G}^*) = \#(A'[A^* \cap H]|\mathfrak{G}') = [A'[A^* \cap H]:A']$ by Th. 16.5 (c), whence there holds $A^* = A'[A^* \cap H]$. We see therefore our assertion $I(\mathfrak{G}') = V(\mathfrak{G}^*) = V(\mathfrak{G}')$.

Elliger [1]; Nagahara [8], [10], [11]; Nagahara-Tominaga [5], [10], [11]; Nobusawa-Tominaga [2]; Tominaga [8], [10], [11].

19. Fundamental theorem of infinite Galois theory

In order to state the fundamental theorem for a left locally finite q-Galois extension A/B in the usual form, we have to add the supplementary assumption $[A:H]_L \leqslant \aleph_0$. Nevertheless, the supplementary assumption will not spoil our project to give a unified Galois theory for simple rings. One may remark further that if A/B is a left locally finite q-Galois extension and $[A:H]_L \leqslant \aleph_0$ then A/B is locally finite and $[A:H] \leqslant \aleph_0$ (Th. 17.16 and Prop. 18.3).

Lemma 19.1. _Let_ A _be q-Galois and left locally finite over_ B, _and_ $[A:H]_L \leqslant \aleph_0$. _If_ A' _is an f-regular intermediate ring of_ A/H _then_ $A'|\mathfrak{G} = \mathfrak{G}(A', A; B)$. _In particular_, $H|\mathfrak{G} = \mathfrak{G}(H/B)$ _and_ A/B _is h-Galois_.

Proof. By Th. 18.8, $[A':H] < \infty$ and $H|\mathfrak{G}(A', A; B) = \mathfrak{G}(H/B)$. Therefore, in case $[A:H]_L < \infty$, the equality is clear. Henceforth, we shall restrict our attention to the case $[A:H]_L = \aleph_0$. Let $\{a_1, a_2, \ldots\}$ be a countably infinite left H-basis of A, and $A_k = H[E, a_1, \ldots, a_k]$ $(k = 1, 2, \ldots)$. Then, $[A_k:H]_L < \infty$ by Th. 18.8. Let τ be an arbitrary element of $\mathfrak{G}(A', A; B)$. As $\infty > [A'\tau:H\tau] = [A'\tau:H]$, there exists a positive integer h_1 such that $A_{h_1} \supset A'\tau$. Then, there exists an element $\sigma \in \mathfrak{G}(A_{h_1}, A; B)$ such that $A'\tau|\sigma = \tau^{-1}$ (Th. 18.8). Repeating the same argument for σ instead of τ, we can find a positive integer $k_1 > h_1$ and $\tau_1 \in \mathfrak{G}(A_{k_1}, A; B)$ such that $A_{k_1} \supset A_{h_1}\sigma$ and $A_{h_1}\sigma|\tau_1 = \sigma^{-1}$. Here, one will readily see that $\tau = A'|\tau_1$ and $A_{k_1}\tau_1 \supset A_{h_1} \supset A'\tau$. Repeating the above procedure for τ_1 instead of τ, we can find positive integers $k_2 > h_2 > k_1$ and $\tau_2 \in \mathfrak{G}(A_{k_2}, A; B)$ such that $\tau_1 = A_{k_1}|\tau_2$ and $A_{k_2}\tau_2 \supset A_{h_2} \supset A_{k_1}\tau_1$. Continuing the same procedure step by step, we obtain inductively positive integers $k_i > h_i > k_{i-1}$ and $\tau_i \in \mathfrak{G}(A_{k_i}, A; B)$ such that $\tau_{i-1} = A_{k_{i-1}}|\tau_i$ and $A_{k_i}\tau_i \supset A_{h_i} \supset A_{k_{i-1}}\tau_{i-1}$ $(A_{k_0} = A', \ \tau_0 = \tau)$. Then, we can define an extension $\bar{\tau} \in \mathfrak{G}(A, A; B)$ of τ by the rule

$A_{k_i}|\bar{\tau} = \tau_i$ $(i = 1, 2, \ldots)$. Since $A\bar{\tau} \supset \bigcup_i A_{h_i} = A$, $\bar{\tau}$ is obviously an automorphism of A. We have proved therefore $\mathfrak{G}(A', A; B) = A'|\mathfrak{G}$. Now, the latter assertion is evident by Cor. 17.12.

Corollary 19.2. *Let* A *be q-Galois and left locally finite over* B, *and* $[V:C_o] \leqslant \aleph_o$. *If* $X = \{x_1, x_2, \ldots\}$ *is a countable subset of* A, *then there exists some* $A' \in \mathfrak{R}/H[X, V]$ *such that* A'/B *is h-Galois and* $[A':H] \leqslant \aleph_o$.

Proof. Let T be in $\mathfrak{R}^{o}_{l.f}$. We set $T_i = T[x_1, \ldots, x_i]$, $A_i' = H[T_i\mathfrak{G}(T_i, A; B), V]$ and $A' = \bigcup A_i'$. Since $[\mathfrak{G}(T_i, A; B)V_R:V_R]_R = [\mathfrak{G}(T_i, A; B)A_R:A_R]_R = [T_i:B] < \infty$ (Prop. 5.7 (b)) and $[V:C_o] \leqslant \aleph_o$, we obtain $[A_i':H] \leqslant \aleph_o$. Hence, noting that $A_i' \subset A_{i+1}'$, it follows then $[A':H]_L \leqslant \aleph_o$. If B' is in $\mathfrak{R}^{o}_{l.f}$ and contained in A' then B' is contained in some A_i', and then one will easily see that $B'\mathfrak{G}(B', A; B) \subset A_i' \subset A'$, namely, $\mathfrak{G}(B', A; B) = \mathfrak{G}(B', A'; B)$. Hence, by Prop. 5.1 (a) and Th. 17.16, we see that A'/B is q-Galois. Accordingly, A'/B is h-Galois by Lemma 19.1.

Now, we arrive at the position to state the following main theorem.

Theorem 19.3. *Let* A *be q-Galois and left locally finite over* B, *and* $[A:H]_L \leqslant \aleph_o$. *Let* A' *be an arbitrary f-regular intermediate ring of* A/B.

(a) *Every* ρ *in* $\mathfrak{G}(A', A; B)$ *can be extended to an automorphism of* A.

(b) A/A' *is h-Galois and locally finite*.

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

Proof. By Th. 18.8 (c), A/A' is q-Galois and locally finite. Accordingly, noting that $[A:V_A^2(A')]_L \leqslant [A:H]_L \leqslant \aleph_o$, (b) is a consequence of Lemma 19.1. Now, let $A'' = A'[H]$. Then, A'' is in $\mathfrak{R}$ (Th. 18.1) and f-regular. Hence, we have $A'|\mathfrak{G} = A'|(A''|\mathfrak{G}) =$

$A'|\mathfrak{G}(A'', A; B) = \mathfrak{G}(A', A; B)$ by Lemma 19.1 and Th. 18.8 (a), which means (a). Finally, (c) is an easy consequence of (b), Cor. 17.12 and Th. 18.12 (a).

In case A/B is an algebraic field extension, it is well known that A/B is Galois if and only if it is normal and separable. The latter of Lemma 19.1 may be regarded as an extension of this fact to simple ring extensions.

Corollary 19.4. *If a division ring A is Galois and left locally finite over a division subring B and $[A:H]_L \leq \aleph_0$ then there exists a 1-1 dual correspondence between closed $(*_f)$-regular subgroups of $\mathfrak{G}$ and f-regular intermediate rings of A/B, in the usual sense of Galois theory.*

An example given by Jacobson [5] shows that Cor. 19.4 is no longer valid for *all* intermediate rings of A/B. (The example was given, in the first place, for the purpose of showing that we can not exclude the assumption $[B:Z] < \infty$ from Th. 7.13.)

Theorem 19.5. *Let A be q-Galois and left locally finite over B, and $[A:H]_L \leq \aleph_0$. Let T be an f-regular intermediate ring of A/B, $\mathfrak{H}$ the group of all B-ring automorphisms of T, $\mathfrak{T} = \{\sigma \in \mathfrak{G};\ T\sigma = T\}$ and $\mathfrak{T}^* = \mathfrak{T}\cdot V(\mathfrak{T})^{\sim}$. If $J(\mathfrak{H}) = B$ then $\mathfrak{T}^*$ is dense in $\mathfrak{G}$, and conversely.*

Proof. By the validity of Th. 19.3, the proof proceeds in the same way as in that of Th. 7.14.

Let A be q-Galois and left locally finite over B, and $[A:H]_L \leq \aleph_0$. As an easy consequence of Th. 19.3, we see that an f-regular intermediate ring T of A/B is $\mathfrak{G}$-invariant if and only if $\mathfrak{G}(T)$ is an invariant subgroup of $\mathfrak{G}$. Moreover, we can prove the next that corresponds exactly to the classical normality theorem.

Corollary 19.6. *Let A be q-Galois and left locally finite over B, and $[A:H]_L \leq \aleph_0$. Let T be an f-regular intermediate ring of A/B. If T/B is Galois and either $T \subset H$ or $V \subset T$ then T is $\mathfrak{G}$-invariant, and the converse is true provided $V \neq (GF(2))_2$.*

Proof. In case $T \subset H$, our assertion is evident by Th. 16.5 (d). While, in case $V \subset T$, $\tilde{V}$ is contained in $\mathfrak{X} = \{\sigma \in \mathfrak{G} ;\ T\sigma = T\}$, and then $\mathfrak{X}$ is dense in $\mathfrak{G}$ (Th. 19.5). Hence, $T\mathfrak{G} = T\mathfrak{X} = T$. The converse is contained in Prop. 8.10.

Finally, we shall prove the following:

Theorem 19.7. *Let A be q-Galois and left locally finite over B, and $[A:H]_L \leqslant \aleph_0$. If T is a $\mathfrak{G}$-invariant f-regular intermediate ring of A/B then the group $\mathfrak{H}$ of all B-ring automorphisms of T is equivalent (i.e. isomorphic and homeomorphic) to $\mathfrak{G}/\mathfrak{G}(T)$.*

Proof. Since $T|\mathfrak{G} = \mathfrak{H}$ (Th. 19.3 (a)), the contraction map ρ: $\sigma \longrightarrow T|\sigma$ is a continuous epimorphism of $\mathfrak{G}$ onto $\mathfrak{H}$ with the kernel $\mathfrak{G}(T)$. In what follows, we shall prove that ρ is an open map. Evidently, T contains $B' \in \mathcal{L}_{l.f}$ such that $V_A(B') = V_A(T)$. Then, A is h-Galois and locally finite over B' (Th. 19.3), $V_A^2(B') \supset T \supset B'$ and T/B' is Galois. Now, for an arbitrary finite subset F of A, choose B'' from $\mathcal{L}_{l.f}/B'[F]$. Then, $T|\mathfrak{G}(B''[T]/B'') = \mathfrak{G}(T/B'' \cap T)$ by Th. 18.1. Since A is h-Galois and locally finite over B'' (Th. 19.3) and $[A:V_A^2(B'')]_L \leqslant \aleph_0$, there holds $\mathfrak{G}(B''[T]/B'') = B''[T]|\mathfrak{G}(B'')$ by Th. 19.3. We obtain therefore $\mathfrak{H}(B'' \cap T) = \mathfrak{G}(T/B'' \cap T) = T|\mathfrak{G}(B'') \subset T|\mathfrak{G}(F)$. As evidently $\mathfrak{H}(B'' \cap T)$ is open, so is $T|\mathfrak{G}(F)$, whence it follows our assertion.

Nagahara [10]; Nagahara-Tominaga [8], [9]; Tominaga [10]; Walter [1].

20. Extensions of compatible pairs

In this section, following Nagahara [10], we shall develop the extension theorems of isomorphisms to obtain more explicit results.

Assume that A/B is q-Galois and left locally finite. Let A_1 be in $\mathfrak{R}$, and A_2 an f-regular intermediate ring of A/B. If $S = A_1 \cap A_2$ is a simple ring such that $V_A(S) = V_A(A_2)$ then A_1 is said to be <u>annexable</u> to A_2. Evidently, A_1 is annexable to every intermediate ring of H/B (Th. 16.5 (a)). If A_1 is annexable to A_2 then A is q-Galois and locally finite over the f-regular intermediate ring S (Th. 18.8 (c)), and then, noting that $S \subset A_2 \subset V_A^2(S) = S[H]$, there holds $A_2 = S[A_2 \cap H]$ and $A_1[A_2] = A_1[A_2 \cap H]$ is in $\mathfrak{R}$ (Th. 18.1). If $\sigma_1 \in \mathfrak{G}(A_1, A; B)$ and $\sigma_2 \in \mathfrak{G}(A_2, A; B)$ are compatible, namely, if $S|\sigma_1 = S|\sigma_2$ then we denote by $\sigma_1 \nabla \sigma_2$ the (not necessarily single valued) mapping of $A_1[A_2]$ into A defined as follows:

$$(\sum a_{k1}^{(1)} a_{k1}^{(2)} \cdots a_{km_k}^{(1)} a_{km_k}^{(2)})(\sigma_1 \nabla \sigma_2) = \sum (a_{k1}^{(1)}\sigma_1)(a_{k1}^{(2)}\sigma_2) \cdots (a_{km_k}^{(1)}\sigma_1)(a_{km_k}^{(2)}\sigma_2),$$

where $a_{kj}^{(i)} \in A_i$ $(i = 1, 2)$. For any subset $\mathfrak{H}_i$ of $\mathfrak{G}(A_i, A; B)$, we set then $\mathfrak{H}_1 \nabla \mathfrak{H}_2 = \{\sigma_1 \nabla \sigma_2;\ \sigma_1 \in \mathfrak{H}_1$ and $\sigma_2 \in \mathfrak{H}_2$ are compatible$\}$. With those notations, we ahve the following proposition which is useful in the subsequent consideration.

Proposition 20.1. <u>Assume that</u> A <u>is q-Galois and left locally finite over</u> B. <u>Let</u> A_1 <u>in</u> $\mathfrak{R}$ <u>be annexable to an f-regular intermediate ring</u> A_2, <u>and</u> $S = A_1 \cap A_2$.

(a) $\mathfrak{G}(A_1[A_2], A; B) = \Gamma(A_1[A_2], A) \cap (\mathfrak{G}(A_1, A; B) \nabla \mathfrak{G}(A_2, A; B))$.

(b) <u>Let</u> $\sigma\nabla\tau$ <u>be in</u> $\mathfrak{G}(A_1, A; B) \nabla \mathfrak{G}(A_2, A; B)$. <u>If</u> $(A_1'|\sigma) \nabla (A_2'|\tau)$ <u>is in</u> $\Gamma(A_1'[A_2'], A)$ <u>for every</u> $A_i' \in \mathfrak{R}_{1.f}$ <u>contained in</u> A_i <u>then</u> $\sigma\nabla\tau$ <u>is in</u> $\mathfrak{G}(A_1[A_2], A; B)$.

(c) <u>If</u> $\mathfrak{G}(A_1[A_2], A; B) = \mathfrak{G}(A_1, A; B) \nabla \mathfrak{G}(A_2, A; B)$ <u>then</u> $A_1|\mathfrak{G}(A_1[A_2], A; B) = \mathfrak{G}(A_1, A; B)$, $A_1|\mathfrak{G}(A_1[A_2], A; A_2) = \mathfrak{G}(A_1, A; S)$ <u>and</u> $A_2|\mathfrak{G}(A_1[A_2], A; A_1) = \mathfrak{G}(A_2, A; S)$.

(d) Assume that $\mathfrak{G}(A_1[A_2], A; B) = \mathfrak{G}(A_1, A; B) \triangledown \mathfrak{G}(A_2, A; B)$. If $S|\mathfrak{G}(A_1, A; B) = \mathfrak{G}(S, A; B)$ then $A_2|\mathfrak{G}(A_1[A_2], A; B) = \mathfrak{G}(A_2, A; B)$, and conversely.

Proof. (a) If ρ is in $\mathfrak{G}(A_1[A_2], A; B)$ then $A_2|\rho \in \mathfrak{G}(A_2, A; B)$ (Cor. 18.4 (b)) and $(A_2 \cap H)\rho \subset H$ (Th. 6.5 (c)), and then $V_A(A_1\rho) = V_A(A_1[A_2 \cap H]\rho) = V_A(A_1[A_2]\rho)$ is simple. Hence, $\mathfrak{G}(A_1[A_2], A; B) \subset \mathfrak{G}(A_1, A; B) \triangledown \mathfrak{G}(A_2, A; B)$. Conversely, if $\sigma \triangledown \tau$ is an isomorphism then $A_1\sigma \in \mathfrak{L}$ and $(A_2 \cap H)\tau \subset H$ yield that $A_1[A_2](\sigma \triangledown \tau) = A_1[A_2 \cap H](\sigma \triangledown \tau) = (A_1\sigma)[(A_2 \cap H)\tau] \in \mathfrak{L}$ (Th. 18.1).

(b) This is an easy consequence of (a) and Th. 6.3.

(c) If σ is in $\mathfrak{G}(A_1, A; B)$ then $S|\sigma = S|\tau$ for some τ in $\mathfrak{G}(A_2, A; B)$ (Cor. 18.4 (b) and Th. 18.8 (a)), and then $\sigma \triangledown \tau \in \mathfrak{G}(A_1[A_2], A; B)$ is an extension of σ. Combining this with (a), we obtain at once the first equality. The other ones will be almost evident.

(d) This can be proved by the similar method as in (c). Conversely, by (c) and Th. 18.8 (a), we obtain $S|\mathfrak{G}(A_1, A; B) = S|(A_1|\mathfrak{G}(A_1[A_2], A; B)) = S|(A_2|\mathfrak{G}(A_1[A_2], A; B)) = S|\mathfrak{G}(A_2, A; B) = \mathfrak{G}(S, A; B)$.

Lemma 20.2. Assume that A is q-Galois and left locally finite over B, and $[A:H]_L \leq \aleph_0$. Let A_1, A_2 be f-regular intermediate rings of A/B, and $S = A_1 \cap A_2$.

(a) The following conditions are equivalent: (1) Every compatible pair (σ_1, σ_2) $(\sigma_i \in \mathfrak{G}(A_i, A; B))$ has a common extension in $\mathfrak{G}$, (2) $\mathfrak{G}(S) = \mathfrak{G}(A_2)\cdot\mathfrak{G}(A_1)$, (2') $\mathfrak{G}(S) = \mathfrak{G}(A_1)\cdot\mathfrak{G}(A_2)$, (3) $A_2|\mathfrak{G}(A_1) = \mathfrak{G}(A_2, A; S)$, and (3') $A_1|\mathfrak{G}(A_2) = \mathfrak{G}(A_1, A; S)$.

(b) If $V_A(S) = V_A(A_2)$ then A_1 is annexable to A_2, and so A is h-Galois and locally finite over S and any of the conditions (1) - (3') in (a) is equivalent with the following: (4) $\mathfrak{G}(A_1[A_2], A; B) = \mathfrak{G}(A_1, A; B) \triangledown \mathfrak{G}(A_2, A; B)$.

Proof. (a) (1)$\Longrightarrow$(2): If σ is in $\mathfrak{G}(S)$ then there exists some $\tau \in \mathfrak{G}(A_1)$ such that $A_2|\tau = A_2|\sigma$. Obviously, $\sigma = (\sigma\tau^{-1})\tau$

and $\sigma\tau^{-1} \in \mathfrak{G}(A_2)$. (2)$\Longrightarrow$(3): By Th. 19.3 (a), $\mathfrak{G}(A_2, A; S) = A_2|\mathfrak{G}(S) = A_2|\mathfrak{G}(A_2)\cdot\mathfrak{G}(A_1) = A_2|\mathfrak{G}(A_1)$. (3)$\Longrightarrow$(1): Let (σ_1, σ_2) be a compatible pair $(\sigma_i \in \mathfrak{G}(A_i, A; B))$. By Th. 19.3 (a), there exists some $\tau_1 \in \mathfrak{G}$ such that $\sigma_1 = A_1|\tau_1$. Since $\gamma = \sigma_2\tau_1^{-1} \in \mathfrak{G}(A_2, A; B) = A_2|\mathfrak{G}(A_1)$, $\gamma = A_2|\tau$ with some $\tau \in \mathfrak{G}(A_1)$, and then $\sigma = \tau\tau_1$ is an extension requested.

(b) Noting that $J(\mathfrak{G}(A_i)) = A_i$ (Th. 19.3 (c)), it follows at once $J(\mathfrak{G}(S)) = S$, which means that $\mathfrak{G}(S)$ is $(*_f)$-regular. Hence, S is f-regular by Th. 18.12 (a). Now, the latter assertions are easy by Th. 19.3 and Prop. 20.1 (a).

Proposition 20.3. <u>Assume that</u> A <u>is q-Galois and left locally finite over</u> B <u>and</u> $[A:H]_L \leqslant \aleph_0$. <u>Let</u> A_1, A_2 <u>be f-regular intermediate rings of</u> A/B <u>such that</u> $V_A(S) = V_A(A_2)$, <u>where</u> $S = A_1 \cap A_2$.

(a) <u>If every compatible pair</u> (σ_1, σ_2) $(\sigma_i \in \mathfrak{G}(A_i, A; B))$ <u>has a common extension in</u> $\mathfrak{G}$ <u>then</u> A_1 <u>is linearly disjoint from</u> A_2.

(b) <u>Assume that</u> A_1 <u>is linearly disjoint from</u> A_2. <u>If</u> $A' \in \mathfrak{R}/S$ <u>is a subring of</u> A_1 <u>left finite over</u> S <u>then</u> $A'|\mathfrak{G}(S) = A'|\mathfrak{G}(A_2)$.

(c) <u>Assume that</u> A_1 <u>is left finite over</u> S. <u>In order that every compatible pair</u> (σ_1, σ_2) $(\sigma_i \in \mathfrak{G}(A_i, A; B))$ <u>have a common extension in</u> $\mathfrak{G}$, <u>it is necessary and sufficient that</u> A_1 <u>be linearly disjoint from</u> A_2.

(d) <u>If</u> A_2 <u>is w-Galois over</u> S <u>then every compatible pair</u> (σ_1, σ_2) $(\sigma_i \in \mathfrak{G}(A_i, A; B))$ <u>has a common extension in</u> $\mathfrak{G}$.

<u>Proof</u>. By Lemma 20.2 (b), A is h-Galois and locally finite over the f-regular intermediate ring S.

(a) Let A' be an arbitrary intermediate ring of A_1/S left finite over S. Then, by Lemma 20.2 (a), $\mathrm{Hom}({}_SA', {}_SA) = A'|\mathrm{Hom}({}_SA, {}_SA) = A'|\mathfrak{G}(S)A_R = A'|\mathfrak{G}(A_1)\cdot\mathfrak{G}(A_2) = A'|\mathfrak{G}(A_2)A_R \subset A'|\mathrm{Hom}({}_{A_2}A, {}_{A_2}A)$, which proves evidently that A_1 is linearly disjoint from A_2 (cf. §19).

(b) Since A/A_2 is h-Galois and locally finite (Th. 19.3 (b)), our assumption yields $\mathrm{Hom}({}_SA', {}_SA) = A'|\mathrm{Hom}({}_{A_2}A_2\cdot A', {}_{A_2}A) = A'|\mathfrak{G}(A_2)A_R$

$= \sum_{\sigma \in \mathfrak{G}(A_2)} (A'|\sigma)A_R$. Now, let τ be an arbitrary element of $\mathfrak{G}(S)$. Then, by Cor. 6.6 (c), $A'|\tau = A'|\sigma\tilde{v}$ for some $\sigma \in \mathfrak{G}(A_2)$ and $v \in V_A(S)^{\cdot} = V_A(A_2)^{\cdot}$. Hence, $A'|\tau$ is contained in $A'|\mathfrak{G}(A_2)$, namely, $A'|\mathfrak{G}(S) = A'|\mathfrak{G}(A_2)$.

(c) This is an easy consequence of (a), (b) and Lemma 20.2 (a).

(d) Since $S \subset A_2 \subset V_A^2(S)$ and A_2/S is Galois, we obtain $A_2|\mathfrak{G}(A_1[A_2]/A_1) = \mathfrak{G}(A_2/S) = \mathfrak{G}(A_2, A; S)$ (Ths. 18.1 (a), 16.5 (d) and 19.3 (a)). Noting that $V_A(A_1[A_2]) = V_A(A_1)$, Th. 16.5 (d) and Th. 19.3 (a) yield $\mathfrak{G}(A_1[A_2]/A_1) = A_1[A_2]|\mathfrak{G}(A_1)$, whence together with the above it follows $A_2|\mathfrak{G}(A_1) = \mathfrak{G}(A_2, A; S)$. Now, our assertion is clear by Lemma 20.2 (a).

Corollary 20.4. *Assume that* A *is q-Galois and left locally finite over* B. *Let* A_1, A_2 *be intermediate rings of* H/B. *If one of the subrings* A_1 *and* A_2 *is Galois over* $A_1 \cap A_2$ *then* $\mathfrak{G}(A_1[A_2], A; B) = \mathfrak{G}(A_1, A; B) \nabla \mathfrak{G}(A_2, A; B)$.

Proof. Since $\mathfrak{G}(A_i, A; B) = \mathfrak{G}(A_i, H; B)$ and $\mathfrak{G}(A_1[A_2], A; B) = \mathfrak{G}(A_1[A_2], H; B)$ (Th. 6.5 (c)) and $\mathfrak{G}(A_1, H; B) \nabla \mathfrak{G}(A_2, H; B) = \mathfrak{G}(A_1[A_2], H; B)$ (Prop. 20.3 (d)), our assertion is evident.

Lemma 20.5. *Assume that* A/B *is q-Galois and left locally finite. Let* A' *be in* $\mathcal{L}$, *and* H^* *an intermediate ring of* H/B. *If* $A' \cap H^* = A' \cap H$ *then* $\mathfrak{G}(A'[H^*], A; B) = \mathfrak{G}(A', A; B) \nabla \mathfrak{G}(H^*, A; B) = \mathfrak{G}(A'[H^{**}], A; B) \nabla \mathfrak{G}(H^*, A; B)$ *for every intermediate ring* H^{**} *of* $H^*/A' \cap H^*$.

Proof. Since $A'[H^{**}] \cap H = H^{**} = (A'[H^{**}] \cap H) \cap H^* = A'[H^{**}] \cap H^*$ (Th. 18.1 (b)), it suffices to prove that every $\sigma \nabla \tau$ in $\mathfrak{G}(A', A; B) \nabla \mathfrak{G}(H^*, A; B)$ is an isomorphism (Prop. 20.1 (a)). By Th. 18.1, $H|\mathfrak{G}(A'[H]/A') = \mathfrak{G}(H/A' \cap H) = \mathfrak{G}(H/A' \cap H^*)$, and so $\mathfrak{G}(H^*, A; A' \cap H^*) = H^*|\mathfrak{G}(H/A' \cap H^*) = H^*|\mathfrak{G}(A'[H]/A') \subset H^*|\Gamma(A'[H^*], A; A')$ (Ths. 6.5 and 16.5). Hence $\mathfrak{G}(H^*, A; A' \cap H^*) = H^*|\mathfrak{G}(A'[H^*], A; A')$, namely, $\mathfrak{G}(A'[H^*], A; A') = \{(A'|1) \nabla \rho';\ \rho' \in \mathfrak{G}(H^*, A; A' \cap H^*)\}$ (Prop. 20.1 (a)). We shall prove first our lemma for the case that $[A':B] < \infty$ and $[H^*:B] < \infty$. Let N^* be a $\mathfrak{G}(H/B)$-invariant shade of H^*, and S^* in $\mathfrak{R}_{l.f}/A'[N^*]$. Then, $\tau = H^*|\tau_o$ for some $\tau_o \in \mathcal{G}(N^*/B)$ and $\sigma = A'|\sigma^*$ for some $\sigma^* \in \mathcal{G}(S^*, A; B)$ (Ths. 6.5 and 16.5). By the remark stated at the beginning of this proof and Th. 16.5, we obtain $H^*|\ \mathcal{G}(A'[H^*], A; A')\sigma^* = \mathcal{G}(H^*, A; A' \cap H^*)\sigma^* \subset \mathcal{G}(H^*, A; A' \cap H^*)\tau_o$. Since $\# \mathcal{G}(H^*, A; A' \cap H^*)\sigma^* = \# \mathcal{G}(H^*, A; A' \cap H^*)\tau_o < \infty$ (Th. 16.5), we have then $H^* \mid \mathcal{G}(A'[H^*], A; A')\sigma^* = \mathcal{G}(H^*, A; A' \cap H^*)\tau_o \ni \tau$. Hence, $\tau = \tau'\sigma^* = H^*|((A'|1) \triangledown \tau')\sigma^*$ for some $\tau' \in \mathcal{G}(H^*, A; A' \cap H^*)$, whence it follows $\sigma \triangledown \tau = ((A'|1) \triangledown \tau')\sigma^* \in \Gamma(A'[H^*], A)$. We shall proceed next in the general case. Let $A'' \in \mathfrak{R}_{l.f}$ be a subring of A', H^{**} an intermediate ring of H^*/B with $[H^{**}:B] < \infty$, and $H^{*\prime}$ an intermediate ring of $H^*/H^{**}[A'' \cap H]$ with $[H^{*\prime}:B] < \infty$. By Th. 6.5 (b), $A''|\sigma \in \mathcal{G}(A'', A; B)$ and $H^{*\prime}|\tau \in \mathcal{G}(H^{*\prime}, A; B)$. Since $A''|\sigma$ and $H^{*\prime}|\tau$ are compatible and $A'' \cap H^{*\prime} = A'' \cap H$, the first step implies $(A''|\sigma) \triangledown (H^{*\prime}|\tau) \in \mathcal{G}(A''[H^{*\prime}], A; B)$. Hence, we obtain $(A''|\sigma) \triangledown (H^{**}|\tau) = A''[H^{**}]|(A''|\sigma) \triangledown (H^{*\prime}|\tau) \in \Gamma(A''[H^{**}], A)$. Our assertion is therefore a consequence of Prop. 20.1 (b).

Corollary 20.6. <u>Assume that</u> A/B <u>is q-Galois and left locally finite</u>. <u>Let</u> A' <u>be in</u> $\mathfrak{R}$, <u>and</u> H^* <u>an intermediate ring of</u> H/B. <u>If one of the subrings</u> H^* <u>and</u> $A' \cap H$ <u>is Galois over</u> $A' \cap H^*$ <u>then</u> $\mathcal{G}(A'[H^*], A; B) = \mathcal{G}(A', A; B) \triangledown \mathcal{G}(H^*, A; B)$.

<u>Proof</u>. Let $\sigma \triangledown \tau$ be in $\mathcal{G}(A', A; B) \triangledown \mathcal{G}(H^*, A; B)$. Since $A' \cap H|\sigma \in \mathcal{G}(A' \cap H, A; B)$ (Cor. 18.4 (b)), there holds $(A' \cap H|\sigma) \triangledown \tau \in \mathcal{G}(A' \cap H, A; B) \triangledown \mathcal{G}(H^*, A; B) = \mathcal{G}((A' \cap H)[H^*], A; B)$ (Cor. 20.4). Moreover, noting that $A' \cap (A' \cap H)[H^*] = A' \cap H$, we obtain $\mathcal{G}(A'[H^*], A; B) = \mathcal{G}(A', A; B) \triangledown \mathcal{G}((A' \cap H)[H^*], A; B)$ (Lemma 20.5). Hence, $\sigma \triangledown ((A' \cap H|\sigma) \triangledown \tau)$ is in $\mathcal{G}(A'[H^*], A; B)$ and coincides with $\sigma \triangledown \tau$, and then our assertion is clear by Prop. 20.1 (a).

Now, we can prove the following:

Theorem 20.7. <u>Assume that</u> A/B <u>is q-Galois and left locally finite</u>. <u>Let</u> $A_1 \in \mathfrak{R}$ <u>be annexable to an f-regular intermediate ring</u> A_2. <u>If one of the subrings</u> A_2 <u>and</u> $A_1 \cap V_A^2(A_2)$ <u>is Galois over</u> $S = A_1 \cap A_2$ <u>then</u> $\mathcal{G}(A_1[A_2], A; B) = \mathcal{G}(A_1, A; B) \triangledown \mathcal{G}(A_2, A; B)$, $A_1|\ \mathcal{G}(A_1[A_2], A; B)$

$= \mathcal{G}(A_1, A; B)$, $A_1 | \mathcal{G}(A_1[A_2], A; A_2) = \mathcal{G}(A_1, A; S)$ <u>and</u> $A_2 | \mathcal{G}(A_1[A_2], A; A_1) = \mathcal{G}(A_2, A; S)$.

<u>Proof</u>. We set $H_2 = A_2 \cap H$. If A_2/S is Galois, then so is $H_2/S \cap H$ (Th. 6.5 (c)). On the other hand, if $A_1 \cap V_A^2(S)/S$ is Galois then $\mathcal{G}(A_1 \cap V_A^2(S)/S) = A_1 \cap V_A^2(S) | \mathcal{G}(V_A^2(S)/S)$ (Th. 16.5), and so $A_1 \cap H | \mathcal{G}(A_1 \cap V_A^2(S)/S) = A_1 \cap H | \mathcal{G}(H/S \cap H)$ (Th. 18.1), whence we obtain $(A_1 \cap H)\mathcal{G}(A_1 \cap V_A^2(S)/S) \subset (A_1 \cap V_A^2(S)) \cap H = A_1 \cap H$, which implies that $A_1 \cap H/S \cap H$ is Galois. Hence, noting that $A_1 \cap H_2 = S \cap H$, Cor. 20.6 yields that $\mathcal{G}(A_1[A_2], A; B) = \mathcal{G}(A_1[H_2], A; B) = \mathcal{G}(A_1, A; B) \nabla \mathcal{G}(H_2, A; B)$. Now, let $\sigma \nabla \tau$ be in $\mathcal{G}(A_1, A; B) \nabla \mathcal{G}(A_2, A; B)$. Then, $\sigma \nabla (H_2|\tau)$ is in $\mathcal{G}(A_1[A_2], A; B)$ and coincides with $\sigma \nabla \tau$. Hence, we obtain $\mathcal{G}(A_1, A; B) \nabla \mathcal{G}(A_2, A; B) = \mathcal{G}(A_1[A_2], A; B)$ (cf. Prop. 20.1 (a)). Accordingly, the others are valid by Prop. 20.1 (c).

Lemma 20.8. <u>Assume that</u> A <u>is q-Galois and left locally finite over</u> B. <u>Let</u> $B' \in \mathcal{R}_{l.f}$. <u>If</u> $s = [B' \cap H:B]$ <u>and</u> $t = [V:V_A(B')]$ <u>then</u> $\mathcal{G}(B', A; B) = \bigcup_1^s \sigma_i \widetilde{V}$ <u>(direct union) and</u> $\sigma_i \widetilde{V} A_R = \bigoplus_{j=1}^t \sigma_i \widetilde{v}_{ij} A_R$ <u>with some</u> $v_{ij} \in V^{\cdot}$.

<u>Proof</u>. At first, we shall prove $\mathcal{G}(B', A; B' \cap H) = B' | \widetilde{V}$. Let B^* be in $\mathcal{R}^{\circ}_{l.f}/B'$, and $H^* = B^* \cap H$. Then, $B' \cap H^* = B' \cap H$. Hence, by Th. 6.5 (c) and the proof of Lemma 20.5, we have $B'[H^*] | \mathcal{G}(B^*, A; B') = \mathcal{G}(B'[H^*], A; B') = \{(B'|1) \nabla \tau;\ \tau \in \mathcal{G}(H^*, A; B' \cap H^*)\}$. Accordingly, $\mathcal{G}(B'[H^*], A; B') = \{ B'[H^*]|\tau_1^*, \dots, B'[H^*]|\tau_{s^*}^*\}$, where $\tau_i^* \in \mathcal{G}(B^*, A; B')$ and $s^* = \# \mathcal{G}(H^*, A; B' \cap H^*) = [H^*:B' \cap H^*]$ (Th. 16.5). Recalling here that $[B^*:H^*] = [V:V_A(B^*)] = [V:V_A(B^*\tau_i^*)]$ (Prop. 18.3) and $[\tau_i^*\widetilde{V}A_R:A_R]_R = [V:V_A(B^*\tau_i^*)]$ (Prop. 5.1 (d)), we readily obtain $\mathcal{G}(B^*, A; B' \cap H) = \mathcal{G}(B^*, A; B' \cap H^*) = \bigcup_1^{s^*} \tau_i^*\widetilde{V}$ (Th. 6.9 (a) and Prop. 5.7). It follows therefore $\mathcal{G}(B', A; B' \cap H) = B' | \mathcal{G}(B^*, A; B' \cap H) = \bigcup_1^{s^*} B'|\tau_i^*\widetilde{V} = B'|\widetilde{V}$ (Th. 6.5 (a)). Now, we shall prove our assertion. If σ, ρ are elements in $\mathcal{G}(B', A; B)$ such that $B' \cap H|\sigma = B' \cap H|\rho$, then

$\rho = \sigma\varepsilon$ with some $\varepsilon \in \mathcal{G}(B'\sigma, A; (B' \cap H)\sigma)$. Since $(B' \cap H)\sigma = B'\sigma \cap H$ by Th. 6.5 (c), the proposition stated at the beginning proves that $\varepsilon = B'\sigma\,|\tilde{v}$. We have seen thus $\mathcal{G}(B', A; B) = \bigcup_1^s \sigma_i\tilde{V}$ (direct union), where $\mathcal{G}(B' \cap H, A; B) = \{B' \cap H|\sigma_1, \dots, B' \cap H|\sigma_s\}$ (Th. 16.5). If $\{v_{i1}, \dots, v_{it}\} \subset V^{\cdot}$ is a right $V_A(B'\sigma_i)$-basis of V (cf. Prop. 18.3), then we readily obtain $\sigma_i\tilde{V}A_R = \sum_{j=1}^t \sigma_i\tilde{v}_{ij}A_R$, and $\mathrm{Hom}({}_BB', {}_BA) = \mathcal{G}(B', A; B)A_R = \sum_{i,j} \sigma_i\tilde{v}_{ij}A_R$. Combining this with $s\cdot t = s\cdot[B':B' \cap H] = [B':B]$ (Prop. 18.3), we obtain at once $\mathrm{Hom}({}_BB', {}_BA) = \oplus_{i=1}^s \oplus_{j=1}^t \sigma_i\tilde{v}_{ij}A_R$.

Proposition 20.9. <u>Assume that</u> A <u>is q-Galois and left locally finite over</u> B. <u>Let</u> $A' \in \mathcal{R}$ <u>be Galois over</u> B. <u>Then,</u> $\mathcal{G}(B', A; B) = B'|\mathcal{G}(A', A; B) = B'|\mathcal{G}(A'/B)V$ <u>for every</u> $B' \in \mathcal{R}_{l.f}$ <u>contained in</u> A', <u>and</u> $\mathcal{G}(A'/B)\tilde{V}$ <u>is dense in</u> $\mathcal{G}(A', A; B)$ (<u>in the finite topology</u>). <u>In particular, if</u> A' <u>contains</u> V <u>then</u> A'/B <u>is h-Galois,</u> $\mathcal{G}(A'/B)$ <u>is dense in</u> $\mathcal{G}(A', A; B)$ <u>and</u> $\mathcal{G}(A', A; B) = \mathcal{G}(A', A'; B)$.

<u>Proof</u>. Obviously, $A' \cap H$ is outer Galois over B and $A' \cap H|\mathcal{G}(A'/B)$ is dense in $\mathcal{G}(A' \cap H/B)$ by Ths. 6.5 (c) and 16.5. Accordingly, noting that $A' \cap H$ is $\mathcal{G}(H/B)$-invariant (Th. 16.5 (d)), we obtain $B' \cap H|\mathcal{G}(B', A; B) = \mathcal{G}(B' \cap H, A; B) = B' \cap H|\mathcal{G}(H/B) = B' \cap H|(A' \cap H|\mathcal{G}(H/B)) = B' \cap H|\mathcal{G}(A' \cap H/B) = B' \cap H|(A' \cap H|\mathcal{G}(A'/B)) = B' \cap H|\mathcal{G}(A'/B)$ (Ths. 6.5 (a) and 16.5). Hence, $\mathcal{G}(B', A; B) = B'|\mathcal{G}(A'/B)\tilde{V} = B'|\mathcal{G}(A', A; B)$ by Lemma 20.8 and Th. 6.5 (b), and so $\mathcal{G}(A'/B)\tilde{V}$ is dense in $\mathcal{G}(A', A; B)$ by Th. 6.5. Next, assume that $A' \supset V$. Since A is $B\cdot V$-A-irreducible (Th. 17.16), A' is $B\cdot V$-A'-irreducible by Prop. 5.1 (a). Hence, A'/B is h-Galois by Cor. 17.12. Now, the latter assertion will be obvious by the former.

We shall conclude this section with the following theorem, which is similar to (and essentially contain) Th. 18.1 (a).

Theorem 20.10. <u>Assume that</u> A <u>is q-Galois and left locally finite over</u> B. <u>Let</u> $A_1 \in \mathcal{R}$ <u>be annexable to an f-regular intermediate ring</u> A_2 <u>of</u> A/B, <u>and</u> $S = A_1 \cap A_2$.

(a) <u>Assume that one of the subrings</u> A_2 <u>and</u> $A_1 \cap V_A^2(S)$ <u>is</u>

Galois over S. *Then, the contraction maps* $\phi: \bar{\sigma} \longrightarrow A_1|\bar{\sigma}$ *of* $\mathfrak{G}(A_1[A_2], A; A_2)$ *and* $\psi: \bar{\tau} \longrightarrow A_2|\bar{\tau}$ *of* $\mathfrak{G}(A_1[A_2], A; A_1)$ *are* 1-1 *onto* $\mathfrak{G}(A_1, A; S)$ *and* 1-1 *onto* $\mathfrak{G}(A_2, A; S)$, *respectively, and* $J(\mathfrak{G}(A_1[A_2], A; A_1)) = A_1$. *If* $A_1'|\mathfrak{G}(A_1, A; S) = \mathfrak{G}(A_1', A; S)$ *for every* $A_1' \in \mathfrak{R}/S$ *contained in* A_1 *such that* $[A_1':S]_L < \infty$, *then* $J(\mathfrak{G}(A_1[A_2], A; A_2)) = A_2$.

(b) *If* A_1 *is Galois over* S *and contains* $V_A(S)$ *then* $A_1 \cap V_A^2(S)/S$ *is outer Galois*, $A_1[A_2]/A_2$ *is h-Galois, and* ϕ *induces an equivalence*: $\mathfrak{G}(A_1[A_2]/A_2) \simeq \mathfrak{G}(A_1/S)$.

(c) *If* A_1 *and* A_2 *are Galois over* B *and* $A_1 \supset V$ *then* $A_1[A_2]/B$ *is h-Galois and* $\mathfrak{G}(A_1[A_2]/B) = \mathfrak{G}(A_1/B) \triangledown \mathfrak{G}(A_2 \cap H/B)$.

(d) *If* A_1 *and* A_2 *are Galois over* S *and* $A_1 \supset V_A(S)$ *then* $A_1[A_2]/S$ *is h-Galois and* $\mathfrak{G}(A_1[A_2]/S) = \mathfrak{G}(A_1/S) \triangledown \mathfrak{G}(A_2/S)$ *is equivalent to the direct product* $\mathfrak{G}(A_1/S) \times \mathfrak{G}(A_2/S)$.

Proof. (a) By Th. 20.7, ϕ and ψ are evidently onto and 1-1. Next, we shall prove the last part. By Th. 18.8 (c), A/S is q-Galois and locally finite. Hence, A_1 contains a subring $U \in \mathfrak{R}/S$ left finite over S such that $U[F] \in \mathfrak{R}$ for every finite subset F of A_1 (Th. 6.3). If a is in $A_1[A_2] \setminus A_2$ then we can find regular intermediate rings A_i' of A_i/S left finite over S such that $a \in A_1'[A_2']$. Obviously, A_1' is annexable to A_2' (Th. 16.5), and then by Th. 18.8 (b), we have $J(\mathfrak{G}(A_1'[A_2'], A; A_2')) = A_2'$. Accordingly, $a\rho' \neq a$ for some $\rho' \in \mathfrak{G}(A_1'[A_2'], A; A_2')$. Since $A_1'|\rho' \in \mathfrak{G}(A_1', A; S)$ by Th. 6.5 (a), by assumption $A_1'|\rho' = A_1'|\rho$ for some $\rho \in \mathfrak{G}(A_1, A; S)$. Then $\bar{\rho} = \rho \triangledown (A_2|1)$ is in $\mathfrak{G}(A_1[A_2], A; A_2)$ (Th. 20.7) and $a\bar{\rho} = a((A_1'|\rho) \triangledown (A_2'|1)) = a\rho' \neq a$, which means $J(\mathfrak{G}(A_1[A_2], A; A_2)) = A_2$. Finally, the validity of Th. 18.8 (a) enables us to apply a similar argument to prove the remainder.

(b) By Th. 18.8 (c), A/S is q-Galois and locally finite. Hence, $A_1 \cap V_A^2(S)/S$ is Galois (Th. 6.5 (c)), and then ϕ is 1-1 and onto $\mathfrak{G}(A_1, A; S)$ by (a). Moreover, we obtain $\mathfrak{G}(A_1[A_2], A; A_2) = \{\sigma \triangledown (A_2|1);\ \sigma \in \mathfrak{G}(A_1, A; S)\}$ (Th. 20.7) and $\mathfrak{G}(A_1, A; S) = \mathfrak{G}(A_1, A_1; S)$ (Prop. 20.9). Hence, we see that an element $\bar{\rho}$ in

$\mathfrak{G}(A_1[A_2], A; A_2)$ is an automorphism if and only if so is $A_1|\bar{\rho}$. If $A_1' \in \mathfrak{R}/S$ is a subring of A_1 left finite over S then $\mathfrak{G}(A_1', A; S) = A_1'|\mathfrak{G}(A_1, A; S) = A_1'|\mathfrak{G}(A_1/S)$ (Prop. 20.9). Hence, for every $a \in A_1[A_2]\backslash A_2$ we can find some $\bar{\rho} \in \mathfrak{G}(A_1[A_2], A; A_2)$ such that $A_1|\bar{\rho} \in \mathfrak{G}(A_1/S)$ and $a\bar{\rho} \neq a$ (cf. the proof of (a)). Then, $\bar{\rho}$ is an automorphism by the above remark, which means that $A_1[A_2]/A_2$ is Galois. Hence, $A_1[A_2]/A_2$ and A_1/S are h-Galois by Prop. 20.9 and Th. 18.8 (c). Finally, the equivalence will be easily seen.

(c) If $H_2 = A_2 \cap H$ then $A_2 = S[H_2]$ and $A_1[A_2] = A_1[H_2]$. Accordingly, noting that H_2/B is Galois by Th. 6.5 (c), we may assume from the beginning that A_2 is contained in H. By Th. 20.7, $\mathfrak{G}(A_1[A_2], A; B) = \mathfrak{G}(A_1, A; B) \nabla \mathfrak{G}(A_2, A; B)$. From $\mathfrak{G}(A_2, A; B) = A_2|\mathfrak{G}(H/B) = \mathfrak{G}(A_2/B)$ (Ths. 6.5 (c) and 16.5) and $\mathfrak{G}(A_1, A; B) = \mathfrak{G}(A_1, A_1; B)$ (Prop. 20.9), it follows then $\mathfrak{G}(A_1[A_2], A; B) = \mathfrak{G}(A_1, A_1; B) \nabla \mathfrak{G}(A_2/B)$. Hence, $\bar{\rho} \in \mathfrak{G}(A_1[A_2], A; B)$ is an automorphism if and only if $A_1|\bar{\rho}$ is an automorphism. Therefore, $\mathfrak{H} = \mathfrak{G}(A_1/B) \nabla \mathfrak{G}(A_2/B)$ is the group of all B-ring automorphisms of $A_1[A_2]$. Since $S|\mathfrak{G}(A_1/B) \subset \mathfrak{G}(S, H; B) = S|\mathfrak{G}(A_2/B)$ (Ths. 6.5 (c) and 16.5), we have $A_1|\mathfrak{H} = \mathfrak{G}(A_1/B)$. Accordingly, noting that $A_1[A_2]/A_1$ is Galois by Th. 18.1, we readily see that $J(\mathfrak{H}) = B$, namely, $A_1[A_2]/B$ is (Galois and so) h-Galois (Prop. 20.9) and $\mathfrak{H} = \mathfrak{G}(A_1[A_2]/B)$.

(d) Since A/S is q-Galois and locally finite (Th. 18.8 (c)), (d) is an easy consequence of (c).

Bialynicki-Birula [1]; Nagahara [10]; Nagahara-Tominaga [8]; Yen [1].

21. $\mathfrak{G}$-locally Galois extension

At first, we shall consider the case that A/B is Galois and $[V:C] < \infty$.

Theorem 21.1. <u>Let</u> A <u>be Galois and left algebraic over</u> B. <u>If</u> $[V:C] < \infty$ <u>then</u> A/B <u>is</u> $\mathfrak{G}$<u>-locally Galois</u>.

<u>Proof</u>. Since A is Galois and finite over H, A is $H \cdot V$-A-irreducible (Th. 6.1). Hence, A/B is h-Galois by Cor. 16.6 (a). If $[B:Z] = \infty$ then A/B is left locally finite by Th. 11.5. While, in case $[B:Z] < \infty$, the local finiteness of A/B is given in Cor. 11.17. Now, let B' be a member of $\mathfrak{L}_{l.f}/\Gamma$ such that $A = B'[H]$. Since $J(B'|\mathfrak{G}) = B$, there exists a finite subset $\mathfrak{f}$ of $\mathfrak{G}$ such that $J(B'|\mathfrak{f}) = B$. If N is an arbitrary $\mathfrak{G}(H/B)$-invariant shade of $B'[\bigcup_{\sigma \in \mathfrak{f}} B'\sigma] \cap H$ then $B'[\bigcup B'\sigma]$ is contained in the simple ring $M = B'[N]$ (Th. 18.1). Moreover, $\mathfrak{H} = \mathfrak{G}(B')[\mathfrak{f}]$ induces an automorphism group of M. Since $J(M|\mathfrak{H}) = B$ (Cor. 6.10) and $V_M(B)$ is simple, M/B is Galois, which means that A/B is locally Galois. Hence, A/B is $\mathfrak{G}$-locally Galois by Cor. 17.13.

As an application of Th. 21.1, we can prove the following:

Theorem 21.2. (a) <u>If</u> A/B <u>is locally Galois then</u> H <u>is simple and for every finite subset</u> F <u>of</u> A <u>there exists an</u> $A' \in \mathfrak{L}/H[F]$ <u>such that</u> $[A':H]_L < \infty$ <u>and</u> A'/B <u>is Galois</u>. <u>The converse is true, provided</u> A/B <u>is left algebraic.</u>

(b) <u>If</u> A/B <u>is locally Galois then so is</u> A/A' <u>for every f-regular intermediate ring</u> A' <u>of</u> A/B.

<u>Proof</u>. (a) By Th. 17.16, H/B is outer Galois and A/H is locally finite. If B' is an arbitrary A/B-shade of $B[E, \Gamma]$ then $A' = B'[H] = \bigcup B'[N_\alpha]$, where N_α ranges over all the $\mathfrak{G}(H/B)$-invariant shades. Now, let B'' be an A/B-shade of $B'[N_\alpha]$, and $\mathfrak{G}' = \{\sigma \in \mathfrak{G}(B''/B);\ B'\sigma = B'\}$. Then, noting that $\mathfrak{G}(B'/B) = B'|\mathfrak{G}'$ (Th. 7.2), Th. 18.1 together with Ths. 6.5 and 16.5 proves that $B'[N_\alpha]/B$ is Galois. Hence, A'/B is locally Galois, and so A'/B is Galois (Th. 19.3 (b)), for $[V_{A'}(B):V_{A'}(A')] = [V_{A'}(H):V_{A'}(A')] \leqslant [A':H]_L < \infty$ by Prop. 5.4. By the same reason, the converse part is

an easy consequence of Th. 21.1.

(b) Choose a subring $B' \in \mathfrak{R}_{1.f}$ of A' such that $V_A(B') = V_A(A')$. Then, A/B' is locally Galois, and then for every finite subset F of A there exists an $A'' \in \mathfrak{R}/V_A^2(B')[F]$ such that A''/B' is Galois and $[V_{A''}(B'):V_{A''}(A'')] \leqslant [A'':V_A^2(B')]_L < \infty$ (see the proof of (a)). Th. 21.1 implies therefore that A''/B' is $\mathfrak{G}(A''/B')$-locally Galois. Since A''/A' is h-Galois and locally finite (Th. 19.3), A''/A' is locally Galois again by Th. 21.1. We have proved therefore that A/A' is locally Galois.

Corollary 21.3. <u>If</u> A/B <u>is locally Galois and</u> $[A:H]_L \leqslant \aleph_0$ <u>then</u> A/A' <u>is</u> $\mathfrak{G}(A')$-<u>locally Galois for every f-regular intermediate ring</u> A' <u>of</u> A/B.

<u>Proof</u>. Since A/A' is h-Galois and locally Galois by Ths. 19.3 and 21.2 (b), our assertion is clear by Cor. 17.13.

Next, we shall consider the case that A/B is Galois and $[V:C_o] < \infty$.

Lemma 21.4. <u>Assume that</u> A <u>is Galois and</u> 2-<u>algebraic over</u> B <u>and</u> $[V:C_o] < \infty$. <u>Let</u> Q <u>be the set of all</u> $q \in A$ <u>such that</u> $B[q] \in \mathfrak{R}^o_{1.f}$. <u>If</u> $B \not\subset C$ <u>then there holds the following</u>:

(a) Q <u>contains an element</u> q' <u>such that</u> H <u>is not contained in the center of</u> $V_A^2(B[q'])$.

(b) <u>There exists an element</u> a <u>such that</u> $H[a] \supset V$ <u>and</u> H <u>is not contained in the center of</u> $H[a]$.

<u>Proof</u>. (a) By the proof of Cor. 8.5, we can easily see $A = B[Q]$. In case $n = 1$, for an arbitrary $b \in B \setminus C$ there exists an element $q' \in A$ such that $bq' \neq q'b$, and then H is not contained in the center of $V_A^2(B[q'])$. While, in case $n > 1$, we may assume that B contains an element $b = \sum x_{ij}e_{ij}$ with $x_{1n} = 1$ and $x_{in} = 0$ for every $i \geqslant 2$ (Prop. 8.3). Then, by Lemma 8.4 (b), $q' = u(E, 1)$ is in Q. Since $bq' \neq q'b$, H is not contained in the center of $V_A^2(B[q'])$.

(b) By (a), there exists some $q' \in Q$ such that H is not contained in the center C' of $A' = V_A^2(B[q'])$. We set $B' = B[q']$.

Case I. $C' \not\subset C_o$: For any $x \in C'\setminus C_o$, there exists some $y \in V$ such that $V = C_o[x, y]$ (Th. 11.16). If $B'' = B'[y] = B[q', y]$ then $A'' = V_A^2(B'') \supset B''[A'] \supset H[x, y] \supset V$. Further, we obtain $\infty > [B'':B]_L \geqslant [V_{A''}(B):V_{A''}(B'')]_R = [V:V_{A''}(A'')]$ (Prop. 5.4). Hence, A'' is inner Galois and finite over H (Th. 7.7). Since $H \not\subset C'$ implies $H \not\subset V_{A''}(A'')$, there exists some a such that $A'' = H[a]$ (Th. 11.16).

Case II. $C' \subset C_o$: Obviously, $V' = V_A(B')$ is a central division algebra over C', and so $V_o = C_o \cdot V' = C_o \otimes_{C'} V'$ is a simple intermediate ring of V/C_o (Props. 4.2 and 4.3) and $V_V^2(V_o) = V_o$ (Th. 7.7). Accordingly, in case $V_o \subsetneqq V$, there holds $C_o \subsetneqq V_V(V_o) = V_V(V') \subset A'$, and hence for an arbitrary $x \in V_V(V_o)\setminus C_o$ there exists an element y such that $V = C_o[x, y]$ (Th. 11.16). Then, by the same argument as in Case I we can find an element a requested. Whereas, in case $V_o = V$, $A'' = A' \cdot V' = A' \otimes_{C'} V'$ is a central simple algebra over C' containing V, for $[V':C'] = [V:C_o] < \infty$. Since $\infty > [B':B]_L \cdot [V':C'] \geqslant [V:V'] \cdot [V':C'] = [V:V_{A''}(A'')]$ by Prop. 5.4, A'' is finite inner Galois over H (Th. 7.7). Now, in the same way as in the last part of Case I, our proof will be completed.

Theorem 21.5. <u>If</u> A <u>is Galois and</u> 2-<u>algebraic over</u> B, <u>and</u> $[V:C_o] < \infty$, <u>then</u> A/B <u>is</u> $\mathfrak{J}$-<u>locally Galois</u>.

<u>Proof</u>. In case $B \subset C$, our theorem is contained in Th. 21.1. Henceforth, we may assume always $B \not\subset C$. Let Q be the set of all $q \in A$ such that $B[q] \in \mathcal{R}^{\circ}_{1.f}$. Then, we can choose a finite subset $Q' = \{ q_1, \dots, q_t \}$ of Q such that $B[F] \subset B[Q']$ (cf. the proof of Lemma 21.4). By Lemma 21.4 (b), there exists an element a_1 such that $A_1 = H[a_1]$ contains V and H is not contained in the center of A_1. If $B_2 = B[a_1, q_1]$ and $A_2 = V_A^2(B_2)$ $(\supset A_1)$ then $\infty > [B_2:B]_L \geqslant [V_{A_2}(B):V_{A_2}(A_2)]$ (Prop. 5.4). Hence, A_2 is finite inner Galois over H. Since $H \not\subset V_{A_1}(A_1)$ implies $H \not\subset V_{A_2}(A_2)$, we can find an element a_2 such that $A_2 = H[a_2]$ (Th. 11.16). Repeating the above argument for $B[a_2, q_2]$ instead of B_2, we obtain a_3 such that $V_A^2(B[a_2, q_2]) = H[a_3]$. Continuing the same procedure step by step, we

obtain eventually $a_2, \ldots, a_{t+1} \in A$ such that $V_A^2(B[a_k, q_k]) = H[a_{k+1}]$ $(k = 1, \ldots, t)$. Noting that $Q' \subset H[a_{t+1}]$, there exists a finite subset F' of H such that $B[Q'] \subset B[F', a_{t+1}]$. Since H/B is outer Galois and left algebraic, there holds $B[F'] = B[h]$ for some $h \in H$ (Th. 16.5 (c)). Hence, it follows $[B[F]:B]_L \leq [B[h, a_{t+1}]:B]_L < \infty$, which means that A/B is left locally finite. Now, let $S = \{s_1, \ldots, s_p\}$ be a C_o-basis of V. If B' is in $\mathscr{R}^{o}_{l.f}/S \cup F$ then $B'|\mathfrak{G} = \cup_1^m (B'|\sigma_i\tilde{V})$ for some $\sigma_i \in \mathfrak{G}$ (Prop. 5.7). We set here $B'' = B'[B'\sigma_1, \ldots, B'\sigma_m]$ and $A'' = V_A^2(B'')$ $(\supset V)$. Noting that $V_A(B'') = V_A(B''[C_o]) = V_A(B''[V])$ and $B''[V]$ is $\mathfrak{G}$-invariant, it is evident that A'' is $\mathfrak{G}$-invariant. Hence, A'' is Galois and left locally finite over B and $[V_{A''}(B):V_{A''}(A'')] \leq [B'':B]_L < \infty$ (Prop. 5.4), so that A''/B is locally Galois by Th. 21.1, which means that A/B is locally Galois. We have proved therefore A/B is $\mathfrak{G}$-locally Galois (Cor. 17.13).

Combining Th. 21.5 with Cor. 19.2, we readily obtain the following:

Corollary 21.6. <u>Let</u> A <u>be left locally finite over a regular subring</u> B, <u>and</u> $[V:C_o] < \infty$. <u>If</u> A/B <u>is q-Galois then it is locally Galois</u>.

Moreover, we can prove the next that contains Prop. 7.16.

Corollary 21.7. <u>Let</u> A <u>be inner Galois and left</u> 2-<u>algebraic over</u> B, <u>and</u> $[V:C_o] < \infty$. <u>Let</u> B' <u>be a simple intermediate ring of</u> A/B <u>left finite over</u> B. <u>If</u> B'/B <u>is inner Galois then the center</u> Z' <u>of</u> B' <u>is contained in</u> Z, <u>and conversely</u>.

Proof. By Th. 21.5, A/B is $\mathfrak{G}$-locally Galois. Hence, A/B' is inner Galois by Th. 17.16 (b). If B'/B is inner Galois then $V_{B'}^2(B) = B$ yields at once $Z' \subset B \cap V = Z$. Now, assume conversely $Z' \subset Z$. Then, V is evidently an algebra over Z'. Since $V_A^2(B') \cap V_A(B') = Z'$, $V_A(B')$ is a central simple algebra of finite rank over Z' (Cor. 7.11). Hence, we obtain $V = V_A(B') \otimes_{Z'} V_{B'}(B)$ (Th. 4.8). From the last relation, we see that $V' = V_{B'}(B)$ is simple. Finally, it follows $J(B'|\tilde{V}') = V_A(V') \cap V_A^2(B') = V_A(V) = B$.

Now, let A_1 and A_2 be intermediate rings of A/B, and $\delta^{(i)}$ in $D(A_i, A; B)$ $(i = 1, 2)$. The pair $(\delta^{(1)}, \delta^{(2)})$ is said to be compatible if $A_1 \cap A_2|\delta^{(1)} = A_1 \cap A_2|\delta^{(2)}$.

Theorem 21.8. Assume that A is Galois and left 2-algebraic over B, and $[V:C_o] < \infty$. Let A_1, A_2 be f-regular intermediate rings of A/B, and $S = A_1 \cap A_2$. In order that every compatible pair $(\delta^{(1)}, \delta^{(2)})$ $(\delta^{(i)} \in D(A_i, A; B))$ have a common extension in $D(A; B)$, it is necessary and sufficient that any of the following equivalent conditions be satisfied: (1) $D(A_1, A; S) = 0$ or $D(A_2, A; S) = 0$, and (2) $V_A(S) = V_A(A_1)$ or $V_A(A_2)$.

Proof. Since A/B is $\mathfrak{J}$-locally Galois (Th. 21.5), the equivalence between (1) and (2) is easy by Th. 6.13 (b). Now, assume that every compatible pair $(\delta^{(1)}, \delta^{(2)})$ has a common extension in $D(A; B)$. Then, for any $\delta \in D(A; S)$ there exists some $\delta^* \in D(A; A_1)$ such that $A_2|\delta^* = A_2|\delta$. Since $\delta - \delta^* \in D(A; A_2)$ and $\delta = \delta^* + (\delta - \delta^*)$, we obtain $D(A; S) = D(A; A_1) + D(A; A_2)$. In particular, if c is an arbitrary element of $V_A(S)$ then $\delta_c = \delta' + \delta''$ $(\delta' \in D(A; A_1)$ and $\delta'' \in D(A; A_2))$. Now, let $B_i \in \mathfrak{L}_{1.f}$ be a subring of A_i with $V_A(B_i) = V_A(A_i)$ $(i = 1, 2)$, and let N be an A/B-shade of $B_1 \cup B_2$. Then, $N|\delta' = N|\delta_{c'}$ and $N|\delta'' = N|\delta_{c''}$ for some $c' \in V_A(B_1)$ and $c'' \in V_A(B_2)$ (Th. 6.13), and then it follows $c = c_o + c' + c''$ with some $c_o \in V_A(N) \subset V_A(A_1) \cap V_A(A_2)$. By the proof of Th. 21.5, we can find a simple subring A^* of A such that $A^* \supset A_1 \cup A_2 \cup V$ and $[V:V_{A^*}(A^*)] < \infty$. If $[V_A(A_1):V_{A^*}(A^*)] \geqslant [V_A(A_2):V_{A^*}(A^*)]$ then $V_A(S) = V_A(A_1) + V_A(A_2)$ implies $[V_A(S):V_A(A_1)]\cdot[V_A(A_1):V_{A^*}(A^*)] < 2\cdot[V_A(A_1):V_{A^*}(A^*)]$, and hence there holds $V_A(A) = V_A(A_1)$, proving (2). Conversely, assume that $V_A(S) = V_A(A_1)$ and $(\delta^{(1)}, \delta^{(2)})$ is compatible. Take an element $v' \in V$ such that $\delta^{(1)} = A_1|\delta_{v'}$ (Th. 6.13). Since $S|\delta^{(2)} = S|\delta^{(1)} = S|\delta_{v'}$, $\delta^{(2)} - A_2|\delta_{v'}$ is contained in $D(A_2, A; S)$. Hence, $\delta^{(2)} - A_2|\delta_{v'} = A_2|\delta_{v''}$ with some $v'' \in V_A(S) = V_A(A_1)$ (Th. 6.13), and $\delta = \delta_{v'} + \delta_{v''}$ is an extension requested.

Combining Th. 21.8 with Prop. 20.3 (d), we readily obtain the next:

Corollary 21.9. Assume that A is Galois and left 2-algebraic over B, $[V:C_o] < \infty$, and $[A:H]_L \leqslant \aleph_0$. Let A_1, A_2 be f-regular intermediate rings of A/B such that $A_1/A_1 \cap A_2$ and $A_2/A_1 \cap A_2$ are w-Galois. If every compatible pair $(\delta^{(1)}, \delta^{(2)})$ $(\delta^{(i)} \in D(A_i, A; B))$ has a common extension in $D(A; B)$ then every compatible pair (σ_1, σ_2) $(\sigma_i \in \mathfrak{G}(A_i, A; B))$ has a common extension in .

Finally, by the way, we shall treat with algebraic extensions of bounded degree. In Cor. 9.7, we have seen that if A/C is algebraic and of bounded degree then A is finite over C. Our principal aim is to prove the same for Galois extensions.

Lemma 21.10. Let B be an intermediate field of A/C. If A/B is left algebraic and of bounded degree then $[A:C] < \infty$.

Proof. At first, we shall prove B/C is algebraic. If not, there exists some $x \in B$ that is transcendental over C, and then $\{1, x_R, x_R^2, \dots\}$ is B_L-free (Prop. 5.1). Now, let X be an arbitrary non-zero B-B-submodule of A with $[X:B]_L < \infty$, $\mu_X(\lambda)$ a minimal polynomial of $X|x_R$ over B_L, and let $n(X)$ be the degree of $\mu_X(\lambda)$. Then, there exists some $u \in A$ such that $u\mu_X(x_R) \neq 0$. If $X_1 = X + BuB$ then $[X_1:B]_L < \infty$ and $n(X_1) > n(X)$. Continuing the same procedure, we can find a B-B-submodule Y of A such that $[Y:B]_L < \infty$ and $n(Y) > m = \max_{a \in A} \{[B[a]:B]_L\}$. As is well known, there exists an element $y \in Y$ such that $\{y, yx_R, \dots, yx_R^{n(Y)-1}\}$ is left B-free (cf. Jacobson [3; p. 69, Th. 1]). But, this implies a contradiction $n(Y) \leqslant [ByB:B]_L \leqslant [B[y]:B]_L \leqslant m$. Secondly, suppose that $[B:C] = \infty$, and take an intermediate field B^* of B/C such that $m < [B^*:C] = k < \infty$. Since A is inner Galois and finite over the simple ring $A^* = V_A(B^*)$ and $V_A(A^*) = B^* \subset A^*$ (Th. 7.7), there exist some $a \in A$ and non-zero $b_1, \dots, b_k \in B^*$ such that $\{a\tilde{b}_1, \dots, a\tilde{b}_k\}$ is a left A^*-basis of A (Cor. 9.5). Recalling here that $B \subset A^*$, the last yields the contradiction $k \leqslant [B[a]:B]_L \leqslant m$, which proves $[B:C] < \infty$. Accordingly, we obtain $[A:C] < \infty$ by Cor. 7.9.

Proposition 21.11. Let A be left algebraic over a simple ring B. Then, the following conditions are equivalent: (1) $[B:Z] < \infty$ and A/B is of bounded degree, (2) $[A:C] < \infty$ and $B\cdot C/B$ is of bounded degree, and (3) $[A:C] < \infty$ and $Z\cdot C/Z$ is of bounded degree.

Proof. Evidently, $B\cdot C = B \otimes_Z Z\cdot C$ and $(2) \Longrightarrow (3)$. $(1) \Longrightarrow (2)$: By Cor. 8.5, we can find some $B' = \sum_1^n D'e'_{ij} \in \mathfrak{L}^{\circ}_{1.f}$ such that $V_A(\{e'_{ij}\})/D'$ is left algebraic and of bounded degree. Since $[D':V_{B'}(B')] < \infty$ (Cor. 7.11), $V_A(\{e'_{ij}\})$ is left algebraic and of bounded degree over the field $V_{B'}(B')\cdot C$. Hence, by Lemma 21.10, $[V_A(\{e'_{ij}\}):C] < \infty$, namely, $[A:C] < \infty$. $(3) \Longrightarrow (1)$: Let $A = \sum_1^s Ca_i$, where $a_1 = 1$. There exists a positive integer k such that every subring of the form $B[c]$ $(c \in C)$ possesses a B-basis consisting of at most k elements of C. Accordingly, if $c_1, \ldots, c_t$ are in C then $B[c_1, \ldots, c_t]$ possesses a B-basis consisting of at most k^t elements of C. In case $B \subset C$, the last yields $[B[x]:B] \leqslant s\cdot k^{s^2+s}$ for every $x \in A$. On the other hand, if $B \not\subset C$ then $A = (B\cdot C)[a]$ with some a (Th. 12.1). There exists therefore a finite subset F of C such that $\{a_1, \ldots, a_s\} \subset B[F, a]$. If $x = \sum_1^s c'_i a_i$ is an arbitrary element of A and $F' = \{c'_1, \ldots, c'_s\}$ $(\subset C)$, it is obvious that $B[x] \subset B[F, F', a]$. Hence, $[B[x]:B]_L \leqslant [B[F, F', a]:B]_L = [B[a]\cdot B[F, F']:B]_L \leqslant [B[a]:B]\cdot k^{s+\#F}$. Finally, $[B:Z] < \infty$ by Cor. 7.11.

Corollary 21.12. Let A be left algebraic and of bounded degree over a simple subring B with $[B:Z] < \infty$. If $Z\cdot C$ is a separable field extension of Z then $[A:B] < \infty$.

Proof. By Th. 21.11, $[A:B]_L \leqslant [A:C]\cdot[Z\cdot C:Z] < \infty$. Since the simple ring $V_A(Z\cdot C)$ coincides with $B \otimes_Z V$ (Ths. 7.7 and 4.8), V is a simple ring. Now, our assertion is a consequence of Prop. 7.12 (b).

Theorem 21.13. If A/B is Galois, left algebraic and of bounded degree, then $[A:B] < \infty$.

Proof. To be easily seen, one may assume that B is a division ring. Since V/Z is Galois, algebraic and of bounded degree, we obtain $[V:Z] = [V:C_o]\cdot[C_o:Z] < \infty$ (Cor. 7.9). In case $[B:Z] < \infty$, our assertion is evidently contained in Cor. 21.12. It remains therefore to prove the case $[B:Z] = \infty$. Then, by Cor. 8.5, there exists a $B' = \sum_1^p Bu_\lambda \in \mathscr{R}^o_{l.f}$. Since $BxB' = (Bx)\sum_1^p Bu_\lambda \subset \sum_1^p B[x]u_\lambda$, we see that $[BxB':B]_L \leqslant mp$ for every $x \in A$, where $m = \max_{y\in A}\{[B[y]:B]_L\}$. Suppose now that $[\mathfrak{G}A_R:A_R]_R = \infty$. Then, for an arbitrary integer $t > mp$, we can find a subset $\{\sigma_1, \dots, \sigma_t\}$ of $\mathfrak{G}$ that is free over A_R (Prop. 5.7). Choose here an arbitrary non-zero B-B'-submodule M_o of A with $[M_o:B]_L < \infty$. If $[\sum_1^t (M_o|\sigma_i)A_R:A_R]_R < t$ (cf. Prop. 5.7), then there holds a non-trivial relation: $\sum_1^t (M_o|\sigma_i)a_{iR} = 0$. Since $\alpha = \sum_1^t \sigma_i a_{iR}$ is non-zero, there exists some $a' \in A$ such that $a'\alpha \neq 0$. Then $M_1 = M_o + Ba'B'$ is left finite over B and $[\sum_1^t (M_o|\sigma_i)A_R:A_R]_R < [\sum_1^t (M_1|\sigma_i)A_R:A_R]_R$. Repeating the same procedure, we can find eventually a B-B'-submodule $M = \sum_1^q Bd_j$ of A such that $\sum_1^t (M|\sigma_i)A_R = \bigoplus_1^t (M|\sigma_i)A_R$. As $[V:Z] < \infty$, $N = \sum_{i,j} (d_j\sigma_i)V$ is a finitely generated right A-submodule of A. Hence, there exist a countably infinite number of non-zero elements $b_1, b_2, \dots$ in B such that $\sum_1^\infty Nb_i = \bigoplus_1^\infty Nb_i$ (Prop. 11.1). Now, let $a = \sum_1^q d_jb_j$ ($\in M$), and $\alpha' = \sum_1^t (M|\sigma_i)v_{iR}$ an arbitrary element of $\bigoplus_1^t (M|\sigma_i)V_R$. Since every $d_j\alpha'$ is in N, $\sum (a\sigma_i)v_i = a\alpha' = \sum (d_j\alpha')b_j \neq 0$. Hence, we have proved that $\{a\sigma_1, \dots, a\sigma_t\}$ is right V-free. We obtain therefore $t\cdot|V| \leqslant [a\mathfrak{G}V_R|V]$. On the other hand, if $M' = BaB'$ then $[a\mathfrak{G}V_R|V] \leqslant [(M'|\mathfrak{G})V_R|V_R] = [(M'|\mathfrak{G})V_R:V_R]_R\cdot|V| \leqslant [M':B]_L\cdot|V| \leqslant mp\cdot|V|$ (Prop. 5.7 (b)). Hence, combining those above, we obtain a contradiction $t \leqslant mp$. We have proved thus $[\mathfrak{G}A_R:A_R]_R < \infty$, so that the two-sided simple ring $\mathfrak{G}A_R$ is simple (cf. § 7). Now, $V_{\mathfrak{A}}(\mathfrak{G}A_R) = B_L$ yields our assertion $[A:B] < \infty$ (Th. 3.11 (a)).

Bialynicki-Birula [1]; Jacobson [6]; Nagahara [5], [6]; Nagahara-Tominaga [4], [6], [8], [9]; Nagahara-Nakajima-Tominaga [1]; Nagahara-Nobusawa-Tominaga [1].

22. Some examples

22a. By Ths. 21.1 and 19.3, we see that if A is Galois and left algebraic over B and $[V:C] < \infty$ then there exists a 1-1 dual correspondence between closed (*)-regular subgroups of $\mathfrak{G}$ and regular intermediate rings of A/B, in the usual sense of Galois theory. However, even in this case, there exists a gap between (*)-regularity and N*-regularity. Prior to giving an example, we shall specialize Th. 18.13 as follows:

Proposition 22.1. Let A be Galois and left algebraic over B, and $[V:C] < \infty$. If $\mathfrak{G}'$ is an N*-regular subgroup of $\mathfrak{G}$ with $I(\mathrm{Cl}\,\mathfrak{G}') = I(\mathfrak{G}')$, then the following conditions are equivalent: (1) $\mathfrak{G}'$ is (*)-regular (and so regular by Th. 18.12), (2) if $\Lambda = \{\ell_k\}$ is a left H-basis of A and $\mathfrak{G}^* = \mathfrak{G}(B[E, \Lambda])$ then $(\mathrm{Cl}\,\mathfrak{G}':(\mathfrak{G}^* \cap \mathrm{Cl}\,\mathfrak{G}')\cdot \widetilde{I(\mathfrak{G}')}) < \infty$, and (3) $(\mathrm{Cl}\,\mathfrak{G}':(\mathfrak{H} \cap \mathrm{Cl}\,\mathfrak{G}')\cdot \widetilde{I(\mathfrak{G}')}) < \infty$ for every open subgroup $\mathfrak{H}$ of $\mathfrak{G}$.

Proof. By Th. 7.7, $[V:C] = [A:H]$ and $V_A^2(I(\mathfrak{G}')) = I(\mathfrak{G}')$. Accordingly, by the validity of Th. 18.13, it is left to prove (2)$\Longrightarrow$(3). Without loss of generality, we may assume here that $\mathfrak{G}'$ is closed and $\mathfrak{H} = \mathfrak{G}(B')$ for some intermediate ring B' of $A/B[E, \Lambda]$ left finite over B. Since $\mathfrak{G}^* \cap \mathfrak{G}'$ is a closed subgroup of the outer group $\mathfrak{G}^* = \mathfrak{G}(A/B[E, \Lambda])$, $T = J(\mathfrak{G}^* \cap \mathfrak{G}')$ is regular and $\mathfrak{G}^* \cap \mathfrak{G}' = \mathfrak{G}(T)$ (Th. 19.3). If $T^* = T[B']$ then $[T^*:T] < \infty$ (Th. 19.3). Hence, by Th. 16.5 (c), we have $(\mathfrak{G}^* \cap \mathfrak{G}':\mathfrak{G}(T^*)) = \#(T^*|(\mathfrak{G}^* \cap \mathfrak{G}')) = [T^*:T] < \infty$, whence it follows that $((\mathfrak{G}^* \cap \mathfrak{G}')\cdot \widetilde{I(\mathfrak{G}')} : \mathfrak{G}(T^*)\cdot \widetilde{I(\mathfrak{G}')}) < \infty$. Noting here that $\mathfrak{H} \subset \mathfrak{G}^*$, we obtain $(\mathfrak{G}':(\mathfrak{H} \cap \mathfrak{G}')\cdot \widetilde{I(\mathfrak{G}')}) = (\mathfrak{G}':(\mathfrak{G}^* \cap \mathfrak{G}')\cdot \widetilde{I(\mathfrak{G}')})\cdot((\mathfrak{G}^* \cap \mathfrak{G}')\cdot \widetilde{I(\mathfrak{G}')} : \mathfrak{G}(T^*)\cdot \widetilde{I(\mathfrak{G}')}) < \infty$.

Corollary 22.2. Let A be Galois and left algebraic over B. If $\mathfrak{G}$ is almost outer then every closed N*-regular subgroup $\mathfrak{G}'$ of $\mathfrak{G}$ is regular.

Proof. In any rate, $[V:C] < \infty$ and $\mathfrak{G}$ is locally finite (Prop. 16.2). If $B^* = B[E, \Lambda]$ and $\mathfrak{G}^* = \mathfrak{G}(B^*)$ (under the notations in Prop. 22.1) then $\infty > \#(H^*|\mathfrak{G}') = (\mathfrak{G}':\mathfrak{G}^* \cap \mathfrak{G}') \geqslant (\mathfrak{G}':(\mathfrak{G}^* \cap \mathfrak{G}')\cdot \widetilde{I(\mathfrak{G}')})$. Hence, $\mathfrak{G}'$ is regular by Prop. 22.1.

Example 22.3. Let C be the algebraic closure of the rational number field P. As is well known, the Galois group $\mathfrak{G}(C/P)$ contains an automorphism σ of infinite order. Now, consider the 2×2 complete matrix ring $A = \sum_1^2 Ce_{ij} = (P)_2 \otimes_P C$ over C with the system of matrix units $E = \{e_{ij}\}$. To be easily seen, A is Galois and locally finite over $B = P$, and $[V:V_A(A)] = [A:C] = 4$, and $\mathfrak{G}(C/P)$ may be naturally regarded as a subgroup of $\mathfrak{G} = \mathfrak{G}(A/B)$. If we set $a = 1 + e_{21}$ then $a^k = 1 + ke_{21}$ for every integer k. Let $\mathfrak{G}'$ be the subgroup $[\sigma\tilde{a}]$ of $\mathfrak{G}$ generated by $\sigma\tilde{a}$. Noting that $\sigma\tilde{a} = \tilde{a}\sigma$ and σ is of infinite order, one will readily see that $\mathfrak{G}'$ is an outer group of infinite order. Moreover, if τ is an arbitrary element of $\mathrm{Cl}\ \mathfrak{G}'$, then for every intermediate rings B_1, B_2 of $A/(P)_2$ with $[B_i:P] < \infty$ there exist integers k_1, k_2 such that $B_i|\tau = B_i|(\sigma\tilde{a})^{k_i}$ $(i = 1, 2)$, whence we have $(P)_2|\tilde{a}^{k_1-k_2} = 1$, namely, $1 + (k_1 - k_2)e_{21} = a^{k_1-k_2} \in P$. Hence, it follows $k_1 = k_2$, which means $\tau = (\sigma\tilde{a})^{k_1} \in \mathfrak{G}'$. Thus, we have seen that $\mathfrak{G}'$ is a closed (outer) N*-regular subgroup of $\mathfrak{G}$. Finally, as $H = V_A^2(B) = C$, $\mathfrak{G}(B[E]) = \mathfrak{G}((P)_2)$ can be taken as $\mathfrak{G}^*$ in Prop. 22.1. If $\tau = (\sigma\tilde{a})^k$ is contained in $\mathfrak{G}^* \cap \mathfrak{G}'$ then $(P)_2|\tilde{a}^k = (P)_2|\tau = 1$ will yield at once $k = 0$, which proves that $\mathfrak{G}^* \cap \mathfrak{G}' = 1$. Accordingly, it follows that $(\mathfrak{G}':(\mathfrak{G}^* \cap \mathfrak{G}')\cdot I(\mathfrak{G}')^{\sim}) = (\mathfrak{G}':1) = \infty$. Hence, $\mathfrak{G}'$ can not be regular by Prop. 22.1.

22b. In Th. 19.3, the existence of Galois correspondence had to be restricted to f-regular intermediate rings. In case A/B is inner Galois and h-Galois, an intermediate ring T of A/B being f-regular is nothing but saying that T is a simple subring left finite over B, and so Th. 19.3 (c) makes essentially no progress than Prop. 6.11. In what follows, we shall deal with a special inner Galois extension of which the Galois group is not locally compact but l.f.d., and for which there exists Galois correspondence between <u>all</u> the closed regular subgroups and <u>all</u> the intermediate rings.

Throughout the subsequent study, we assume always that A <u>is</u>

$\mathfrak{G}$-locally Galois over a field B and $\mathfrak{G}$ is abelian. Under this situation, the latter part of Cor. 9.5 (b) is still valid.

Proposition 22.4. *If* A *is* $\mathfrak{G}$-*locally Galois over a field* B *and* $\mathfrak{G}$ *is abelian, then either* A *is a field or* B *coincides with* V, *and so every intermediate ring of* A/B *is simple*.

Proof. By Cor. 17.13, A/B is Galois. In case $\mathfrak{G}$ is outer, the commutativity of A has been shown in Cor. 4.9. Therefore, in what follows, we may restrict our attention to the case $V \neq C$. Let v be an arbitrary element in $V \setminus C$. Then, there exists some $a \in A$ such that $va \neq av$. Now, for every $w \in V$, we can find a $\mathfrak{G}$-shade A' of $B[a, v, w]$. Since $\mathfrak{G}(A'/B)$ ($\subset A'|\mathfrak{G}$) is abelian and $V_{A'}(B)$ does not coincide with the center of A', $V_{A'}(B) = B$ by Cor. 9.5 (b), which proves evidently $V = B$. The simplicity of every intermediate ring is then a consequence of Cor. 6.2.

In what follows, we assume further that A *is non-commutative,* namely, A is inner Galois over the maximal subfield B (Prop. 22.4). We shall introduce here the following conditions:

(i) If C' is an intermediate field of B/C with $[B:C'] < \infty$, and T an intermediate ring of A/B with $V_T(T) \subset C'$, then there exists an intermediate ring B' of T/B such that $V_{B'}(B') \subset C'$ and $[B':B] < \infty$.

(ii) If C' is an intermediate field of B/C then there exists a family $\{C'_\alpha\}$ of intermediate fields C'_α of B/C such that $[B:C'_\alpha] < \infty$ and $\bigcap_\alpha C'_\alpha = C'$.

(iii) If C' is an intermediate field of B/C with $[B:C'] < \infty$ then $[C'':C' \cap C''] < \infty$ for every intermediate field C'' of B/C.

If T and T' are arbitrary (simple) intermediate rings of A/B then $V_A(T) = V_{T'}(T) = V_B(T)$, and $J(T|\widetilde{B}) = B$, and hence T/B is always inner Galois. In particular, if $[T:B] < \infty$ then $[T:V_T(T)] = [B:V_T(T)]^2 = [T:B]^2 < \infty$.

Lemma 22.5. *Let* $A \neq C$ *be* $\mathfrak{G}$-*locally Galois over a field* B, *and let* $\mathfrak{G}$ *be abelian. Let* C' *be an intermediate field of* B/C *with*

$[B:C'] < \infty$, and T an intermediate ring of A/B with $V_T(T) \subset C'$. Assume the condition (i). If T' is an arbitrary intermediate ring of A/T then $V_{T'}(C')$ is a central simple algebra of finite rank over C'.

Proof. By the condition (i), there exists an intermediate ring B' of T/B such that $V_{B'}(B') \subset C'$ and $[B':B] < \infty$. Then, by the above remark, we have $[B':V_{B'}(B')] < \infty$, and so $V_{B'}^2(C') = C'$. Hence, the center of $B'' = V_{B'}(C')$ coincides with C'. If $B^* = V_{T'}(C')$ $(\supset B'')$ then $C' \subset V_{B^*}(B^*) \subset V_{B^*}(B'') = V_{B''}(B'') = C'$, namely, $V_{B^*}(B'') = V_{B^*}(B^*) = C'$. We obtain therefore $\infty > [B'':C'] = [B'':V_{B^*}(B^*)] = [B^*:V_{B^*}(B'')] = [B^*:C']$.

Theorem 22.6. Let $A \neq C$ be $\mathfrak{G}$-locally Galois over a field B, and let $\mathfrak{G}$ be abelian. If the conditions (i), (ii) and (iii) are satisfied then there exists a 1-1 dual correspondence between closed regular subgroups of $\mathfrak{G}$ and intermediate rings of A/B, in the usual sense of Galois theory.

Proof. Let T be an arbitrary intermediate ring of A/B, and x arbitrary element of $T' = V_A^2(T)$. If $T_1 = B[x]$ and $C_1 = V_{T_1}(T_1)$ then $\infty > [T_1:B] = [B:C_1]$. Noting that $C_1 = V_{T'}(T_1) \supset V_{T'}(T') = V_T(T') = V_T(T)$, we see that $V_{T'}(C_1)$ and $V_T(C_1)$ are central simple algebras of finite rank over C_1 (Lemma 22.5). Hence, $[B:C_1]$ coincides with $[V_T(C_1):B]$, and so x is contained in $V_{T'}(C_1) = V_T(C_1) \subset T$. We have proved thus $V_A^2(T) = T$. Next, we shall prove that $V_A^2(C') = C'$ for every intermediate field C' of B/C. By the condition (ii), there exists a family $\{C'_\alpha\}$ of intermediate fields C'_α of B/C such that $[B:C'_\alpha] < \infty$ and $\bigcap_\alpha C'_\alpha = C'$. Since every $V_A(C')$ is a central simple algebra (of finite rank) over C' (Lemma 22.5), $C'_\alpha = V_A^2(C'_\alpha) \cap V_A(C'_\alpha) = V_A^2(C'_\alpha)$. It follows therefore $C' \subset V_A^2(C') \subset \bigcap_\alpha V_A^2(C'_\alpha) = \bigcap_\alpha C'_\alpha = C'$, namely, $V_A^2(C') = C'$. Finally, we shall prove that A/T is left locally finite. Let F be an arbitrary finite subset of A. If we set $T^* = B[F]$ and $C^* = V_{T^*}(T^*)$, then $[B:C^*] = [T^*:B] < \infty$. Accordingly, if $C'' = V_T(T) = V_A(T)$ then $[C'':C^* \cap C''] < \infty$ by the condition (iii). Since the center of $T_1 = V_A(C^* \cap C'')$ coincides with $V_A^2(C^* \cap C'') = C^* \cap C''$ by the second assertion given above, we obtain $[T_1:V_{T_1}(C'')] =$

$[C'':C^* \cap C''] < \infty$. Recalling here that $T_1 \supset V_A(C'') = V_A^2(T) = T$ by the first assertion given above, it is evident that $T = V_A(C'') = V_{T_1}(C'')$. We obtain therefore $[T_1:T] = [C'':C^* \cap C'']$. Since T_1 contains obviously T^* as well as T, it follows then $[T[F]:T]_L \leq [T_1:T] < \infty$, which proves the left local finiteness of A/T. Since A is B-A-irreducible by Th. 6.1, A is T-A-irreducible much more. Accordingly, A/T is h-Galois by Cor. 17.12, and so $\mathfrak{G}(T) = \mathrm{Cl}\ V_A(T)^{\sim}$ by Th. 18.12.

Example 22.7. In what follows, we shall present an example promised at the opening of this subsection. By G. Köthe [1], there exist a countably infinite number of (non-commutative) central division algebras A_i of finite rank over the rational number field C such that $[A_i:C]$ and $[A_j:C]$ are relatively prime for every $i \neq j$. Since every A_i is a cyclic division algebra over C (Brauer-Hasse-Noether [1]), A_i contains a maximal subfield B_i that is a cyclic extension of C. Then, $A^{(i)} = A_1 \otimes_C \cdots \otimes_C A_i$ is a central division algebra over C (Cor. 4.4). If $i \leq j$ then by the canonical isomorphism $A^{(i)}$ may be regarded as a division subalgebra of $A^{(j)}$, and so we may consider the central division algebra $A = \varinjlim A^{(i)}$ over C. Obviously, $B^{(i)} = B_1 \otimes_C \cdots \otimes_C B_i$ is a maximal subfield of $A^{(i)}$, and then $B = \varinjlim B^{(i)}$ is a maximal subfield of A. Since $B_1, B_2, \ldots$ are independent over C as subfields of B (namely, the intersection of every B_i with the composite of all B_j's except B_i is C and the composite of all B_j's is B), we shall write $B = \prod_1^\infty B_i$. Evidently, $J(\tilde{B}) = B$, $[A:B] = \aleph_0$, and there exist an infinite number of non-f-regular intermediate rings of A/B. If F is an arbitrary finite subset of A, F is contained in some $A^{(i)}$, so that $B[F] \subset A^{(i)} \otimes_C Z^{(i)}$, where $Z^{(i)} = \prod_{i+1}^\infty B_\nu$. Hence, $[B[F]:B]_L \leq [A^{(i)} \otimes_C Z^{(i)}:B] < \infty$, which proves the left local finiteness of A/B. Accordingly, $\mathfrak{G}$ is not locally compact (Prop. 16.3) but l.f.d. (Prop. 16.4). In below, we shall show that the above extension A/B satisfies the conditions (i), (ii) and (iii) introduced above. Every $\mathfrak{G}_i = \mathfrak{G}(B_i/C)$ can be regarded naturally as a subgroup of $\mathfrak{G}^{(\nu)} = \mathfrak{G}(B^{(\nu)}/C)$

for $\nu \geqslant i$, and then $\mathfrak{G}^{(\nu)}$ and $\mathfrak{G}_i^{(\nu)} = \mathfrak{G}(B^{(\nu)}/B_i)$ coincides with the cyclic group $\mathfrak{G}_1 \times \cdots \times \mathfrak{G}_\nu$ and $\mathfrak{G}_1 \times \cdots \times \check{\mathfrak{G}}_i \times \cdots \times \mathfrak{G}_\nu$, respectively. Now, let C^* be an arbitrary intermediate field of $B^{(\nu)}/C$, and $\mathfrak{H} = \mathfrak{G}(B^{(\nu)}/C^*)$. Then, the Galois group $\mathfrak{H}\cdot\mathfrak{G}_i^{(\nu)}$ of $B^{(\nu)}/C^* \cap B_i$ coincides with $(\mathfrak{H} \cap \mathfrak{G}_i) \times \mathfrak{G}_i^{(\nu)}$, and then it follows that $\mathfrak{H} = \bigcap_{i=1}^{\nu} (\mathfrak{H} \cap \mathfrak{G}_i) \times \mathfrak{G}_i^{(\nu)}$. Hence, we obtain $C^* = (C^* \cap B_1) \otimes_C \cdots {}_C\otimes (C^* \cap B_\nu)$. If C' is an arbitrary intermediate field of B/C then $C' = \prod_1^\infty (C' \cap B_i)$. In fact, for every $c' \in C'$, $C^* = C[c']$ is contained in some $B^{(\nu)}$, and so the above remark shows that $C^* = (C^* \cap B_1) \otimes_C \cdots \otimes_C (C^* \cap B_\nu)$, whence we readily obtain $C' = \prod_1^\infty (C' \cap B_i)$. In what follows, this fact will be used freely without mention. Obviously, B is finite over $C'_\alpha = \prod_1^\alpha (C' \cap B_i) \otimes_C Z^{(\alpha)}$ and $C' = \prod_1^\infty (C' \cap B_i) = \bigcap_1^\infty C'_\alpha$, which proves (ii). Now, assume that $[B:C'] < \infty$. Then, $C' = \prod_1^j (C' \cap B_i) \otimes_C Z^{(j)}$ for some sufficiently large j, and so for any intermediate field C'' of B/C there holds $C'' \cap C' = \prod_1^j (C'' \cap C' \cap B_i) \otimes_C \prod_{j+1}^\infty (C'' \cap B_i)$. Recalling that $C'' = \prod_1^j (C'' \cap B_i) \otimes_C \prod_{j+1}^\infty (C'' \cap B_i)$, we readily obtain $[C'' : C'' \cap C'] < \infty$, proving (iii). Finally, we shall prove (i). Let T be an arbitrary intermediate ring of A/B. If we set $T_\nu = (A^{(\nu)} \otimes_C Z^{(\nu)}) \cap T$ then $T = \bigcup_1^\infty T_\nu$, and so $V_T(T) = \bigcap_1^\infty V_T(T_\nu) = \bigcap_1^\infty V_{T_\nu}(T_\nu)$. Since $V_{T_\nu}(T_\nu) \supset V_{T_{\nu+1}}(T_{\nu+1})$, we obtain $B_i \supset B_{1i} \supset B_{2i} \supset \cdots (\supset C)$, where $B_{\nu i} = V_{T_\nu}(T_\nu) \cap B_i$. However, as $\bigcap_{\nu=1}^\infty B_{\nu i} = (\bigcap_1^\infty V_{T_\nu}(T_\nu)) \cap B_i = V_T(T) \cap B_i$ and $[B_i : C] < \infty$, there exists an integer ν_i such that $B_{\nu' i} = V_T(T) \cap B_i$ for every $\nu' > \nu_i$. Accordingly, if $\mu > \max\{\nu_1, \ldots, \nu_j\}$ then $V_{T_\mu}(T_\mu) = \prod_{i=1}^\infty B_{\mu i} \subset (V_T(T) \cap B_1) \otimes_C \cdots \otimes_C (V_T(T) \cap B_j) \otimes_C Z^{(j)} \subset C'$. This together with $[T_\mu : B] < \infty$ shows the validity of (i).

Köthe [1]; Moriya-Nagahara-Tominaga [1]; Nagahara-Tominaga [8]; Tominaga [12].

Bibliography

Albert, A. A. [1]: Structure of algebras. Amer. Math. Soc. Colloq. Publ. 24, 1939; [2]: Two element generation of a separable algebra. Bull. Amer. Math. Soc. 50, 786-788 (1944).

Amitsur, S. A. [1]: Non-commutative cyclic fields. Duke Math. J. 21, 87-105 (1954); [2]: Invariant submodules of simple rings. Proc. Amer. Math. Soc. 7, 987-989 (1956).

Artin, E. [1]: Galois theory. Notre Dame 1942.

Artin, E. Nesbitt, G. and R. Thrall [1]: Rings with minimum condition. University of Michigan 1944.

Artin, E. and G. Whaples [1]: The theory of simple rings. Amer. J. Math. 65, 87-107 (1943).

Asano, S. [1]: On invariant subspaces of division algebras. Kodai Math. Sem. Rep. 18, 322-334 (1966); [2]: On the automorphism rings of division algebras. Kodai Math. Sem. Rep. 18, 368-372 (1966).

Azumaya, G. [1]: New foundation of the theory of simple rings. Proc. Japan Acad. 22, 325-332 (1946); [2]: Galois theory for uniserial rings. J. Math. Soc. Japan 1, 130-146 (1951); [3]: Algebraic theory of simple rings. Tokyo 1951 (in Japanese); [4]: Completely faithful modules and self-injective rings. Nagoya Math. J. 27, 697-708 (1966).

Azumaya, G. and T. Nakayama [1]: On irreducible rings. Ann. of Math. 48, 949-965 (1947); [2]: Algebra II (Theory of rings). Tokyo 1954 (in Japanese).

Bialynicki-Birula, A. [1]: On automorphisms and derivations of simple rings with minimum condition. Trans. Amer. Math. Soc. 98, 468-484 (1961).

Bortfeld, R. [1]: Ein Satz zur Galoistheorie in Schiefkörper. J. f. d. reine u. angew. Math. 201, 196-206 (1959).

Bourbaki, N. [1]: Algèbre, Chap. III. Algèbre multilinéaire. Hermann, Paris, 1948; [2]: Algèbre, Chap. VIII. Modules et anneaux semi-simples. Hermann, Paris, 1958; [3]:Topologie générale, Chap. I. Structures topologiques - Chap. II. Structures uniformes. Hermann, Paris 1951.

Brauer, R. [1]: On a theorem of H. Cartan. Bull. Amer. Math. Soc. 55 619-620 (1949).

Brauer, R., Hasse, H. and E. Noether [1]: Beweis eines Hauptsatzes in der Theorie der Algebren. J. f. d. reine u. angew. Math. 167, 399-404 (1932).

Cartan, H. [1]: Extension de la théorie de Galois aux corps non commutatifs. C. R. Acad. Sci. Paris 224, 87-89 (1947); [2]: Les principaux théorèmes de la théorie de Galois pour les corps non necessairement commutatifs. C. R. Acad. Sci. Paris 224, 249-251 (1947); [3]: Théorie de Galois pour les corps non commutatifs. Ann. École Norm. Sup. 64, 59-77 (1947).

Cartan, H. and S. Eilenberg [1]: Homological algebra. Princeton 1956.

Chase, S. U., Harrison, D. K. and A. Rosenberg [1]: Galois theory and Galois cohomology of commutative rings. Memoirs Amer. Math. Soc. 52, 1965.

DeMeyer, F. R. [1]: Some note on the general Galois theory of rings. Osaka J. Math. 1, 117-127 (1964); [2]: Galois theory in separable algebras over commutative rings. Ill. J. Math. 10, 287-295 (1966).

Dieudonné, J. [1]: La théorie de Galois des anneaux simples et semisimples. Comment. Math. Helv. 21, 154-184 (1948).

Eilenberg, S. and N. Steenrod [1]: Foundations of algebraic topology. Princeton 1952.

Elliger, S. [1]: Über das Rangproblem bei Körpererweiterungen. J. f. d. reine u. angew. Math. 221, 162-175 (1966).

Faith, C. C. [1]: Extensions of normal bases and completely basic fields. Trans. Amer. Math. Soc. 85, 406-427 (1957); [2]: Galois extensions in what every element with regular trace is a normal basis element. Proc. Amer. Math. Soc. 9, 222-229 (1958); Correction. Ibid. 11, 670 (1960); [3]: On conjugates in division rings. Can. J. Math. 10, 374-380 (1958); [4]: Abelian Galois groups. Proc. Amer. Math. Soc. 10, 767-774 (1959); [5]: Zwei-Elemente-Erzeugung und Endlichkeit der Dimension von Divisionsalgebren. Archiv der Math. 11, 405-406 (1960).

Hattori, A. [1]: On invariant subrings. Jap. J. Math. 21, 121-129 (1951); [2]: On the multiplicative group of simple algebras and orthogonal groups of three dimensions. J. Math. Soc. Japan 4, 205-217 (1952).

Hirata, K. and K. Sugano [1]: On semisimple extensions and separable extensions over non commutative rings. J. Math. Soc. Japan 18, 360-373 (1966).

Hochschild, G. [1]: Automorphisms of simple algebras. Trans. Amer. Math. Soc. 69, 292-301 (1950).

Hua, L. K. [1]: Some properties of a sfield. Proc. Nat. Acad. Sci. USA. 35, 533-537 (1949).

Inatomi, A. [1]: On generating elements of simple algebras. Kodai Math. Sem. Rep. 14, 149-159 (1962); [2]: Remark on Galois theory of simple rings. Kodai Math. Sem. Rep. 14, 160-161 (1962).

Jacobson, N. [1]: The theory of rings. Amer. Math. Soc. Math. Surveys 1, New York 1943; [2]: A note on division rings. Amer. J. Math. 69, 27-36 (1947); [3]: Lectures in abstract algebra, II. Linear algebra. New York 1953; [4]: Lectures in abstract algebra, III. Theory of fields and Galois theory. New York 1964; [5]: A note on two dimensional division ring extensions. Amer. J. Math. 77, 593-599 (1955); [6]: Structure of rings. Amer. Math. Soc. Colloq. Publ. 37, 1956; [7]: Generation of separable and central simple algebras. J. Math. Pures et Appl., Ser. IX. 36, 217-227 (1957).

Janusz, G. J. [1]: Separable algebras over commutative rings. Trans. Amer. Math. Soc. 122, 461-479 (1966).

Kanzaki, T. [1]: On commutor rings and Galois theory of separable algebras. Osaka J. Math. 1, 103-115 (1964); [2]: On Galois extension of rings. Nagoya Math. J. 27, 43-49 (1966).

Kasch, F. [1]: Über den Satz vom primitiven Element bei Schiefkörpern. J. f. d. reine u. angew. Math. 189, 150-159 (1951); [2]: Zur Erzeugung separabler Algebren. Norsk Mat. Tidsskr. 34, 97-99 (1952); [3]: Ein Satz über den Endomorphismenring eines Vektorraums. Archiv der Math. 3, 434-435 (1952); [4]: Invariante Untermoduln des Endomorphismenrings eines Vektorraums. Archiv der Math. 4, 182-190 (1953); [5]: Halblineare Abbildungen und die Rangrelation bei Galoisschen Erweiterungen. Archiv der Math. 4, 402-407 (1953); [6]: Über den Endomorphismenring eines Vektorraumes und den Satz von Normalbasis. Math. Ann. 126, 447-463 (1953); [7]: Grundlagen einer Theorie der Frobeniuserweiterungen. Math. Ann. 127, 453-474 (1954); [8]: Ein Bemerkung über innere Automorphismen. Math. J. Okayama Univ. 6, 131-133 (1957).

Kasch, F. and H. Tominaga [1]: On generating elements of simple rings. Proc. Japan Acad. 33, 187-189 (1957).

Kishimoto, K. [1]: Some remarks on Cartan-Brauer-Hua theorem. J. Fac. Sci. Hokkaido Univ. Ser. I. 15, 219-220 (1961); [2]: On cyclic extensions of simple rings. J. Fac. Sci. Hokkaido Univ., Ser. I. 19, 74-85 (1966); [3]: On polynomial extensions of simple rings. J. Fac. Sci. Hokkaido Univ., Ser. I. 19, 169-180 (1966).

Kishimoto, K., Nagahara, T. and H. Tominaga [1]: Supplementary remarks to the previous papers. Math. J. Okayama Univ. 11, 159-163 (1963); Errata. Ibid. 12, 169 (1966).

Kishimoto, K., Onodera, T. and H. Tominaga [1]: On the normal basis theorems and the extension dimension. J. Fac. Sci. Hokkaido Univ., Ser. I. 18, 81-88 (1964).

Köthe, G. [1]: Schiefkörper unendlichen Ranges uber dem Zentrum. Math. Ann. 105, 14-39 (1931).

Kreimer, H. F. [1]: A Galois theory for noncommutative rings. Trans. Amer. Math. Soc. 127, 29-41 (1967); [2]: Galois theory for noncommutative rings and normal bases. Trans. Amer. Math. Soc. 127, 42-49 (1967).

Krull, W. [1]: Galois Theorie der unendlichen algebraischen Erweiterungen. Math. Ann. 100, 687-698 (1928).

Masuda, K. [1]: Automorphisms of algebras and a theorem concerning norms. Math. J. Okayama Univ. 12, 39-47 (1963).

Miyashita, Y. [1]: Finite outer Galois theory of non-commutative rings. J. Fac. Sci. Hokkaido Univ., Ser. I. 19, 115-134 (1966); [2]: Locally finite outer Galois theory. J. Fac. Sci. Hokkaido Univ., Ser. I. 20, 1-26 (1967).

Moriya, M. [1]: Zur Galoisschen Theorie der Schiefkörper. Math. J. Okayama Univ. 9, 49-62 (1959).

Moriya, M. and T. Nagahara [1]: On generating elements of Galois extensions of division rings II. Math. J. Okayama Univ. 7, 89-94 (1957).

Moriya, M., Nagahara, T. and H. Tominaga [1]: A note on Galois theory of division rings. Math. J. Okayama Univ. 7, 83-88 (1957).

Nagahara, T. [1]: On primitive elements of Galois extensions of division rings. Math. J. Okayama Univ. 6, 23-28 (1956); [2]: On generating elements of Galois extensions of division rings. Math. J. Okayama Univ. 6, 181-190 (1957); [3]: III. Math. J. Okayama Univ. 7, 173-178 (1957); [4]: IV. Math. J. Okayama Univ. 8, 181-188 (1958); [5]: V. Math. J. Okayama Univ. 10, 11-17 (1960); [6]: On algebraic Galois extensions of simple rings. Math. J. Okayama Univ. 11, 59-65 (1962); [7]: On generating elements of Galois extensions of simple rings. Proc. Japan Acad. 38, 611-614 (1962); [8]: On Galois conditions and

Galois groups of simple rings. Trans. Amer. Math. Soc. 116, 417-434 (1965); [9]: A note on Galois theory of commutative rings. Proc. Amer. Math. Soc. 18, 334-340 (1967); [10]: Quasi-Galois extensions of simple rings. Math. J. Okayama Univ. 12, 107-146 (1966); [11]: Supplements to the previous paper "Quasi-Galois extensions of simple rings". Math. J. Okayama Univ. 12, 159-166 (1966); [12]: On N-groups of automorphisms in division rings. Math. J. Okayama Univ. 13, 29-34 (1967); [13]: On N-regular groups of automorphisms in simple rings. 13, 129-149 (1968).

Nagahara, T. and H. Tominaga [1]: A note on Galois theory of division rings of infinite degree. Proc. Japan Acad. 31, 655-658 (1955); [2]: On Galois theory of division rings. Proc. Japan Acad. 32, 153-156 (1956); [3]: On Galois theory of division rings. Math. J. Okayama Univ. 6, 1-21 (1956); [4]: II. Math. J. Okayama Univ. 7, 169-172 (1957); [5]: Some remarks on Galois extensions of division rings. Math. J. Okayama Univ. 9, 5-8 (1959); [6]: On Galois and locally Galois extensions of simple rings. Math. J. Okayama Univ. 10, 143-166 (1961); [7]: Corrections and supplements to the previous paper "On Galois and locally Galois extensions of simple rings". Math. J. Okayama Univ. 11, 67-77 (1963); [8]: On Galois theory of simple rings. Math. J. Okayama Univ. 11, 79-117 (1963); Errata. Ibid. 12, 167 (1966); [9]: Some theorems on Galois theory of simple rings. J. Fac. Sci. Hokkaido Univ., Ser. I. 17, 1-13 (1963); [10]: On quasi-Galois extensions of division rings. J. Fac. Sci. Hokkaido Univ., Ser. I. 17, 73-78 (1963); [11]: On dimensions of simple ring extensions. J. Fac. Sci. Hokkaido Univ., Ser. I. 19, 162-168 (1966); [12]: Algebraic extensions of simple rings II. Math. J. Okayama Univ. 13, 23-28 (1967).

Nagahara, T., Nakajima, A. and H. Tominaga [1]: Algebraic extensions of simple rings I. Math. J. Okayama Univ. 13, 15-22 (1967).

Nagahara, T., Nobusawa, N. and H. Tominaga [1]: Galois theory of simple rings IV. Math. J. Okayama Univ. 8, 189-194 (1958).

Nagahara, T., Onodera, T. and H. Tominaga [1]: On normal basis theorem and strictly Galois extensions. Math. J. Okayama Univ. 8, 133-142 (1958).

Nakayama, T. [1]: Normal basis of a quasi-field. Proc. Imp. Acad. Tokyo 16, 532-536 (1940); [2]: Semilinear normal basis for quasifields. Amer. J. Math. 71, 241-248 (1949); [3]: Galois theory for general rings with minimum condition. J. Math. Soc. Japan 1, 203-216 (1949); [4]: Generalized Galois theory of rings with minimum condition I. Amer. J. Math. 73, 1-21 (1951); [5]: II. Amer. J. Math. 77, 1-16 (1955); [6]: Non-normal Galois theory for non-commutative and non-semi-simple rings. Can. J. Math. 3, 208-218 (1951); [7]: Automorphisms of simple, completely primitive, and directly indecomposable rings. Ann. of Math. 55, 538-551 (1952); [8]: Galois theory of simple rings. Trans. Amer. Math. Soc. 73, 276-292 (1952); [9]: On a generalized notion of Galois extensions of a ring. Osaka Math. J. 15, 11-25 (1963).

Nobusawa, N. [1]: An extension of Krull's Galois theory to division rings. Osaka Math. J. 7, 1-6 (1955); [2]: On compact Galois groups of division rings. Osaka Math. J. 8, 43-50 (1956); [3]: A note on Galois extensions of division rings. Math. J. Okayama Univ. 7, 179-183 (1957).

Nobusawa, N. and H. Tominaga [1]: Some remarks on strictly Galois extensions of simple rings. Math. J. Okayama Univ. 9, 13-17 (1959); [2]: On Galois theory of division rings III. Math. J. Okayama Univ. 10, 67-73 (1960).

Ôhori, M. and H. Tominaga [1]: A note on non-commutative Kummer extensions. J. Fac. Sci. Hokkaido Univ., Ser. I. 18, 78-80 (1964).

Onodera, T. [1]: On semilinear normal basis. J. Fac. Sci. Hokkaido Univ., Ser. I. 18, 23-33 (1964).

Onodera, T. and H. Tominaga [1]: On strictly Galois extensions of degree p^e over a division ring of characteristic p. Math. J. Okayama Univ. 7, 77-81 (1957); [2]: A note on strictly Galois extensions of primary rings. J. Fac. Sci. Hokkaido Univ., Ser. I. 15, 193-194 (1961).

Rosenberg, A. and D. Zelinsky [1]: Galois theory of continuous transformation rings. Trans. Amer. Math. Soc. 79, 429-452 (1955); [2]: Extensions of derivations in continuous transformation rings. Trans. Amer. Math. Soc. 79, 453-458 (1955).

Scott, W. R. [1]: On the multiplicative group of a division ring. Proc. Amer. Math. Soc. 8, 303-305 (1957).

Shoda, K. [1]: Über die Galoissche Theorie der halbeinfachen hyperkomplexen Systemen. Math. Ann. 107, 252-258 (1932/33).

Takeuchi, Y. [1]: On Galois extension over a commutative rings. Osaka J. Math. 2, 137-145 (1965); [2]: Infinite outer Galois theory of non commutative rings. Osaka J. Math. 3, 195-200 (1966).

Tominaga, H. [1]: On a theorem of N. Jacobson. Proc. Japan Acad. 31, 653-654 (1955); [2]: Galois theory of simple rings. Math. J. Okayama Univ. 6, 29-48 (1956); [3]: II. Math. J. Okayama Univ. 6, 153-170 (1957); [4]: A note on conjugates. Math. J. Okayama Univ. 7, 75-76 (1957); [5]: II. Math. J. Okayama Univ. 9, 1-3 (1959); [6]: A note on Galois theory of primary rings. Math. J. Okayama Univ. 8, 117-123 (1958); [7]: On automorphism groups of finite order in division rings. J. Fac. Sci. Hokkaido Univ., Ser. I. 15, 195-197 (1961); [8]: On Nagahara's theorem. J. Fac. Sci. Hokkaido Univ., Ser. I. 18, 153-157 (1965); [9]: Note on extensions of derivations in simple rings. J. Fac. Sci. Hokkaido Univ., Ser. I. 19, 56-57 (1965); [10]: On q-Galois extensions of simple rings. Nagoya Math. J. 27, 485-507 (1966); [11]: Note on q-Galois extensions of simple rings. J. Fac. Sci. Hokkaido Univ., Ser. I. 19, 66-70 (1966); [12]: On Galois extensions over a field and abelian Galois groups. Math. J. Okayama Univ. 12, 153-158 (1966); [13]: Some results on normal bases. Math. J. Okayama Univ. 13, 111-118 (1968).

Van der Waerden, B. L. [1]: Moderne Algebra Bd. 1, 2nd ed., Berlin 1937; [2]: Bd. 2. 2nd ed., Berlin 1940.

Villamayor, O. E. and D. Zelinsky [1]: Galois theory for rings with finitely many idempotents. Nagoya Math. J. 27, 721-731 (1966).

Walter, J. H. [1]: On the Galois theory of division rings. Proc. Amer. Math. Soc. 10, 898-907 (1959).

Yen, Ti [1]: Isomorphisms of simple rings. Can. J. Math. 15, 467-470 (1963).

Index

A

algebraic 13
almost outer 114
annexable 152

B

bounded degree 48

C

capacity 12
completely basic 72
completely faithful 7
completely reducible 3
correct subgroup 71

D

DF-group 45

F

faithful 3
F-group 45
f-regular 41

G

Galois 43
Galois group 43

H

h-Galois 42
$\mathfrak{H}$-Kummer extension 68
$\mathfrak{H}$-locally Galois 117
$\mathfrak{H}$-n.b.e. 63
$\mathfrak{H}$-regular 62
homogeneous component 3
homogeneously completely reducible 3

I

idealistic decomposition 3
inner Galois 47
inverse limit 1
irreducible 3

K

k-algebraic 13

L

l.f.d. 116
locally finite (extension) 13
locally finite (group) 114
locally Galois 117

N

N-group 45
N-regular 45
N*-group 45
N*-regular 45

O

outer Galois 47

P

pre-q-system 122
primitive 11
projective 6

Q

q-Galois 42
q-system 122
q_o-system 121
quaternion algebra 72

R

radical 18
reduced order 45
regular (group) 46
regular (module) 8
regular (subring) 24

S

semi-simple 18
separable 21
shade 117
simple 10
singly generated 77
socle 4
standard identity 17
(*)-regular 46
$(*_f)$-regular 142

T

trace ideal 7
trivial extension 97
two-sided simple 10

U

unital (module) 3
unital (subring) 6
upper distinguished 8

V

$\widetilde{V}$-subset 121

W

w-Galois 43
w-q-Galois 32