ARITHMETIC OF GROUP REPRESENTATIONS

SHUICHI TAKAHASHI

(Received January 15, 1959)

Let $\mathfrak{G}$ be a finite group, k be an algebraic field of finite degree over the field of rationals $\mathbf{Q}$. In a representation space V over k we consider a $\Gamma = \mathfrak{o}[\mathfrak{G}]$-lattice (Gitter) M in V which is a regular $\mathfrak{o}$-right module and $\mathfrak{G}$-left module where $\mathfrak{o}$ is the ring of integers in k. The set of all Γ-lattices which we denotes by $\{M;\ k/\mathfrak{o}\}$ can be classified into Γ-isomorphic Γ-lattices in the following way:

$$\{M;\ k/\mathfrak{o}\} = \{M_1;\ \mathfrak{o}/\mathfrak{o}\} + \cdots\cdots\cdots + \{M_c;\ \mathfrak{o}/\mathfrak{o}\}.$$

If $k = \mathbf{Q}$ is the field of rationals and V is irreducible, this class number is always finite and was proved by C. Jordan [13][1].

In the book of Speiser [20] this theorem was proved only in two special cases, namely, $\mathfrak{G}$ is a cyclic group or V is absolutely irreducible. The reason for this may be explained by the following considerations.

Let $\mathfrak{p}$ be a finite or infinite prime. We can consider $\mathfrak{p}$-extension $M_\mathfrak{p}$ of the Γ-lattice M and put

$$\{M_\mathfrak{p};\ k_\mathfrak{p}/\mathfrak{o}_\mathfrak{p}\} = \{M_\mathfrak{p}^{(1)};\ \mathfrak{o}_\mathfrak{p}/\mathfrak{o}_\mathfrak{p}\} + \cdots\cdots\cdots + M_\mathfrak{p}^{(j)};\ \mathfrak{o}_\mathfrak{p}/\mathfrak{o}_\mathfrak{p}\}.$$

The local class number $j = j(\mathfrak{p})$ is always finite and $= 1$ if $\mathfrak{p}$ does not divide the order $g = \# \mathfrak{G}$ of the group $\mathfrak{G}$.

If we define genus of M as

$$\{M;\ \tilde{\mathfrak{o}}/\mathfrak{o}\} = \bigcap_{\mathfrak{p}} \{M;\ \mathfrak{o}_\mathfrak{p}/\mathfrak{o}_\mathfrak{p}\}$$

then the number of genera in all Γ-lattices in V is

$$j = \prod_{\mathfrak{p} | g} j(\mathfrak{p})$$

and is finite (§7). If M is absolutely irreducible we have

$$c = j \qquad (\S\ 10).$$

On the other hand, number of classes in a genus is expressible as a kind of class number of a suitable algebraic group (§9), which was considered by T. Ono [17] and its finiteness was proved for commutative case by him. Simple considerations show that if $\mathfrak{G}$ is cyclic and $k = \mathbf{Q}$

1) Number in the bracket refers to the bibliography at the end of this paper.

$$j = 1$$
$$c = h$$

where h is the class number of the field of g-th roots of unity. General cases are somewhat complicated but relate with class number of a suitable algebraic extension K/k (§11).

After this investigation was almost completed, the author found papers by Maranda [15], [16]. He introduced the concept of genus and its product formula (§§7-8), but his definition is a global one and its locality and hence equality with my definition was not proved by him.

Finally, I must express my hearty thanks to Prof. Tannaka for his kind advices and encouragement during the preparation of this paper.

CONTENTS

NOTATIONS

$\mathfrak{G}$: finite group.
k: algebraic number field of finite degree over the rational field $\mathbf{Q}$.
$\mathfrak{o}$: ring of integers in k.
$\Gamma = \mathfrak{o}[\mathfrak{G}]$: group ring of $\mathfrak{G}$ over $\mathfrak{o}$.
V: vector space of dimension m over k; mostly Γ-space.
$A(x)$: representation of $\mathfrak{G}$ by $GL(V; k)$.
M: lattice in V; mostly Γ-lattice.

1. Preliminaries on lattices (Gitter). By a lattice in an algebraic field k we mean an $\mathfrak{o}$-module M contained in a definite vector spacc V over k such that

1) M is a finitely generated $\mathfrak{o}$-module,
2) M generates over k the vector space V i.e. $Mk = V$.

Or, equivalently, a lattice is a regular $\mathfrak{o}$-module i. e.

1′) M' is a finitely generated $\mathfrak{o}$-module,
2′) $u \in M'$, $\alpha \in \mathfrak{o}$, $u\alpha = 0$ imply $u = 0$ or $\alpha = 0$.

Namely, a lattice M in former sense is of course a regular $\mathfrak{o}$-module and regular $\mathfrak{o}$-module M' is a lattice contained in the vector space $M'k = V'$ of k-extension of M'.

Let $\mathfrak{p}$ be a prime in k. Assume first $\mathfrak{p}$ is finite. $k_\mathfrak{p}$, $\mathfrak{o}_\mathfrak{p}$ denote respectively $\mathfrak{p}$-adic completion of k and $\mathfrak{p}$-adic integers in $k_\mathfrak{p}$. If M is a lattice in k, then its $\mathfrak{p}$-adic extension

$$M_\mathfrak{p} = M\mathfrak{o}_\mathfrak{p}$$

is a lattice contained in the vector space $V_\mathfrak{p} = Vk_\mathfrak{p}$. For infinite prime $\mathfrak{p}_\infty$, we simply put

$$M_{\mathfrak{p}\infty} = V_{\mathfrak{p}\infty}$$

in accordance with the convention $\mathfrak{o}_{\mathfrak{p}\infty} = k_{\mathfrak{p}\infty}$

PROPOSITION 1. 1. *If M is a lattice contained in V, then*

$$M = \bigcap_{\mathfrak{p}} (V \cap M_\mathfrak{p})$$

where the intersection extends over all finite and infinite primes in k.

A proof is found in Eichler[2] [10] and almost clear if we assume Stenitz's basis theorem[3].

PROPOSITION 1. 2. *Let $v_1, \ldots\ldots v_m$ be an arbitrary k-basis of V. Then for any lattice M in V we have*

$$M_\mathfrak{p} = v_1\mathfrak{o}_\mathfrak{p} \oplus \ldots\ldots \oplus v_m\mathfrak{o}_\mathfrak{p}$$

except for a finite number of primes in k.

For, by Steinitz's basis theorem

$$M = u_1\mathfrak{o} \oplus \ldots\ldots \oplus u_{m-1}\mathfrak{o} \oplus u_m\mathfrak{a}$$

with an ideal $\mathfrak{a}$ in k. For a prime not in $\mathfrak{a}$ we have

$$M_\mathfrak{p} = u_1\mathfrak{o}_\mathfrak{p} \oplus \ldots\ldots \oplus u_m\mathfrak{o}_\mathfrak{p}.$$

Since $(u_1, \ldots\ldots u_m)$ and $(v_1, \ldots\ldots v_m)$ are two k-basis of V, they are connected by a regular matrix in k which is $\mathfrak{p}$-unimodular (i. e. a matrix in $\mathfrak{o}_\mathfrak{p}$ whose determinant is a $\mathfrak{p}$-unit) except for a finite number of primes in k.

PROPOSITION 1. 3. *To each prime $\mathfrak{p}$ put $M^{(\mathfrak{p})}$ for a lattice in $V_\mathfrak{p}$ such that except for a finite number of primes*

2) Eichler [10], §12, Satz 12. 1.
3) For example: Eichler [10], §12, Satz 12. 5.

$$M^{(\mathfrak{p})} = v_1\mathfrak{o}_\mathfrak{p} \oplus \cdots\cdots \oplus v_m\mathfrak{o}_\mathfrak{p}$$

where $v_1, \cdots\cdots v_m$ *is a k-basis of V. Then the intersection*

$$M = \bigcap_\mathfrak{p} (V \cap M^{(\mathfrak{p})})$$

over all primes in k, is a lattice in V such that

$$M_\mathfrak{p} = M^{(\mathfrak{p})}$$

for all primes in k.

PROOF. Put $M' = v_1\mathfrak{o} \oplus \cdots\cdots \oplus v_m\mathfrak{o}$. Since $M'_\mathfrak{p} = M^{(\mathfrak{p})}$ except for a finite number of primes. We can fined $\gamma, \gamma' \in \mathfrak{o}$ such that

$$M^{(\mathfrak{p})}\ \gamma \subseteqq M'_\mathfrak{p} \subseteqq M^{(\mathfrak{p})}\ \gamma'$$

for all primes in k. From $M \subseteqq M'\ \gamma^{-1}$, M is a finite $\mathfrak{o}$-module. On the other hand, $M' \subseteqq M\gamma$ implies $Mk = V$. Therefore M is a lattice in V. Next, $M \subseteqq M^{(\mathfrak{p})}$ implies $M_\mathfrak{p} \subseteqq M^{(\mathfrak{p})}$ for all primes in k. Take $u \in M^{(\mathfrak{p})}$ arbitrarily, put $u_1, \cdots\cdots u_n$ $(n \geqq m)$ for an $\mathfrak{o}$-generator of M, secured by first part of the proof. We have

$$u = u_1\alpha_1 + \cdots\cdots + u_n\alpha_n$$

with $\alpha_i \in k_\mathfrak{p}$.
From approximation theorem on valuations, we can take $\beta_i \in k$ such that

$$\beta_i \equiv \alpha_i \ (\mathfrak{o}_\mathfrak{p})$$
$$\beta_i \equiv 0 \ (\mathfrak{o}_{\mathfrak{p}'}) \text{ for all primes } \mathfrak{p}'(\neq \mathfrak{p}) \text{ in } k.$$

Then

$$v = u_1\beta_1 + \cdots\cdots + u_n\beta_n$$

is a vector in V such that it is contained in $M^{(\mathfrak{p})}$ and $M^{(\mathfrak{p}')}$ for any prime $\mathfrak{p}' \neq \mathfrak{p}$, i. e.

$$v \in \bigcap_\mathfrak{p} (V \cap M^{(\mathfrak{p})}) = M.$$

On the other hand, we have

$$u = v + \sum_{i=1}^n u_i(\alpha_i - \beta_i)$$

with $v \in M$, $\alpha_i - \beta_i \in . \mathfrak{o}_\mathfrak{p}$. This means $\sum_{i=1}^n u_i(\alpha_i - \beta_i) \in M_\mathfrak{p}$ and finally $u \in M_\mathfrak{p}$. q e. d.

2. **Representations by lattices.** Let $\mathfrak{G}$ be a finite group and $\Gamma = \mathfrak{o}[\mathfrak{G}]$ be the group ring over $\mathfrak{o}$. Assume now V is a Γ-left space over k. Any element $x \in \mathfrak{G}$ is represented by an automorphism

$$A(x) \in GL(V; k)$$

of the vector space V. Symbolically $xV = VA(x)$.

By a Γ-lattice in V, we mean a lattice M such that

$$MA(x) \subseteq M$$

for all $x \in \mathfrak{G}$.

To a Γ-lattice M we can associate a finite set of matrix representations in the following way. Let $v_1, \ldots\ldots v_m$ be a k-basis of V, since M is a lattice in V by Prop. 1.2, except for a finite system of primes $\mathfrak{p}_1, \ldots\ldots \mathfrak{p}_r$ we have

$$M_{\mathfrak{p}} = v_1\mathfrak{o}_{\mathfrak{p}} \oplus \ldots\ldots \oplus v_m\mathfrak{o}_{\mathfrak{p}}.$$

For exceptional $\mathfrak{p}_i$ $(i = 1, \ldots\ldots r)$ we can put

$$M_{\mathfrak{p}_i} = v_{i1}\mathfrak{o}_{\mathfrak{p}_i} \oplus \ldots\ldots \oplus v_{im}\mathfrak{o}_{\mathfrak{p}_i} \qquad i = 1, \ldots\ldots r$$

since $\mathfrak{o}_{\mathfrak{p}_i}$ are principal ideal domains.

Put

$$xv_i = \sum_{j=1}^{m} v_j a_{ji}^0(x) \qquad a_{ji}^0(x) \in k$$

$$xv_{ij} = \sum_{l=1}^{m} v_{il} a_{lj}^i(x) \qquad a_{lj}^i(x) \in \mathfrak{o}_{\mathfrak{p}_i}$$

then matrices:

$$A_i(x) = (a_{lj}^i(x)) \qquad i = 0, 1, \ldots\ldots r$$

are $(r+1)$-matrix representations of the group $\mathfrak{G}$ such that $A_i(x)$ $(i = 1, \ldots\ldots, r)$ are $k_{\mathfrak{p}_i}$-equivalent to $A_0(x)$. Notice that the elements $a_{ij}^0(x) \in k$ are integral for all prime $\mathfrak{p} \neq \mathfrak{p}_i (i = 1, \ldots\ldots r)$.

Conversely given a matrix representation $A_0(x)$ in k and $\mathfrak{p}_i$-adic integral matrix representations $A_i(x)$ $(i = 1, \ldots\ldots, r)$ which are $k_{\mathfrak{p}_i}$-equivalent to $A_0(x)$ for any prime $\mathfrak{p}_i$ for which $A_0(x)$ is not necessarily $\mathfrak{p}_i$-integral. Then we can fined a Γ-lattice M whose associated matrix representations are given $A_i(x)$ $(i = 0, 1, \ldots\ldots, r)$. Namely, if $v_1, \ldots\ldots, v_m$ be a k-basis of the vector space V, we put

$$M^{(\mathfrak{p})} = v_1\mathfrak{o}_{\mathfrak{p}} \oplus \ldots\ldots \oplus v_m\mathfrak{o}_{\mathfrak{p}} \qquad \mathfrak{p} \neq \mathfrak{p}_i \ (i = 1, \ldots\ldots, r)$$

with $\mathfrak{G}$-left operation:

$$xv_i = \sum_{j=1}^{m} v_j a_{ji}^0(x)$$

where $(a_{ji}^0(x)) = A_0(x)$. For an exceptional prime $\mathfrak{p}_i$ let R_i be a regular matrix in $k_{\mathfrak{p}_i}$ such that

$$A_i(x) = R_i^{-1} A_0(x) R_i$$

and put

$$M^{(\mathfrak{p}_i)} = v_{ij}\mathfrak{o}_{\mathfrak{p}_i} \oplus \cdots\cdots \oplus v_{im}\mathfrak{o}_{\mathfrak{p}_i}$$

where

$$(v_{i1}, \cdots\cdots, v_{im}) = (v_1, \cdots\cdots, v_m)R_i$$

is a $k_{\mathfrak{p}_i}$-basis of $V_{\mathfrak{p}_i}$.
Then by Prop. 1. 3

$$M = \bigcap_{\mathfrak{p}} (V \cap M^{(\mathfrak{p})})$$

is a desired Γ-lattice in V.

3. Reducibility of representations. We consider now reducibility of a Γ-lattice M in connection with reducibility of matrix representation by the vector space $V = Mk$.

LEMMA 1. *Let M, N be two regular $\mathfrak{o}$-modules. Then we have*

$$(M \cap N)k = Mk \cap Nk.$$

PROOF. From $M \cap N \subseteq M$ *and* $M \cap N \subseteq N$, it is obvious that

$$(M \cap N)\, k \subseteq Mk \cap Nk.$$

Let $a\alpha = b\beta \in Mk \cap Nk$ with $a \in M$, $b \in N$, α, $\beta \in k$ be given. Take $\gamma \in \mathfrak{o}$ such that $\alpha\gamma \in \mathfrak{o}$, $\beta\gamma \in \mathfrak{o}$, then $a\alpha\gamma = b\beta\gamma \in M \cap N$ and $a\alpha = (a\alpha\gamma)\cdot\gamma^{-1} \in (A \cap B)k$. q. e. d.

We say that a submodule N of a regular $\mathfrak{o}$-module M is primitive in M if one of the following, equivalent, condition is satisfied:

1) $Nk \cap M = N$,
2) Quotient module M/N also is a regular $\mathfrak{o}$-module,
3) $a \in M$, $a\alpha \in N$ with $\alpha \in k$. $\alpha \neq 0$ imply $a \in N$.

LEMMA 2. *If N is a primitive submodule of A, then naturally*

$$(M/N)k \simeq Mk/Nk,$$

PROOF. The map $\varphi: M/N \rightarrow Mk/Nk$ defined naturally by $\varphi(a) = a$ for $a \in M$ is into isomorphic by the primitivity of N in M. (e. g. by 3)). Therefore it remains to show that M/N contains as many linearly independent elements as that of Mk/Nk. But this is obvious since any elements $a_1, \cdots\cdots a_r$ of M that are linearly independent mod Nk are a priori linearly independent mod N. q. e. d.

Now we define reducibility of a Γ-lattice M as follows:

M is reducible if it contains a primitive submodule N neither 0 nor M such that N itself is also a Γ-lattice in $Nk = W$.

PROPOSITION 3.1. *A Γ-lattice M is reducible if and only if the matrix representation defined by $V = Mk$ is reducible.*

PROOF. Assume first M is reducible, then there exists a primitive submodule N. Nk is a subspace of $Mk = V$ neither 0 nor V by primitivity of N in M. Of course Nk is a Γ-space and therefore V is reducible.

Next, let $Mk = V$ be reducible, then there exists a Γ-subspace $W \subset V$ different from 0 or V. Put $N = W \cap M$. As a submodule of M, N is a regular $\mathfrak{o}$-module. By lemma 1 $Nk = W$, it follows that N is a primitive submodule of M. Since N is a Γ-module, M is reducible. q. e. d.

4. Some cohomology groups. Let $A_1(x)$, $A_2(x)$ be two representations of the group $\mathfrak{G}$ by matrices of degree r, s respectively with elements in a commutative ring R with unity element. We now define cohomology groups $H^n(\mathfrak{G} : A_1, A_2)$ as follows:
n-cochains are functions $E(x_1, \cdots, x_n)$ from $\mathfrak{G} \times \cdots\cdots \times \mathfrak{G}$ (n-factors) to $R_{r,s}$ where $R_{s,r}$ denotes the set of all matrices consist of r-rows and s-columns with elements in R.
Coboundary operations are defined by

$$\begin{aligned}\delta E(x_1, \ldots\ldots, x_{n+1}) = {} & A_1(x_1)E(x_2, \ldots\ldots, x_{n+1}) \\ & + \sum_{i=1}^{n}(-1)^i E(x_1, \ldots\ldots, x_i x_{i+1}, \ldots\ldots x_{n+1}) \\ & + (-1)^{n+1} E(x_1, \ldots\ldots, x_n) A_2(x_{n+1}) \\ & \qquad n = 0, 1, 2, \ldots\ldots\end{aligned}$$

From these, cohomology groups are defined as usual

$$H^n(\mathfrak{G}\,;\, A_1, A_2) = n\text{-cocycle}/n\text{-coboundary} \qquad n = 0, 1, 2, \ldots\ldots$$

Obviously,

PROPOSITION 4.1. *The set $H^0(\mathfrak{G}\,;\, \mathrm{A}_1, A_2)$ consist of all intertwinning matrices E between A_1, A_2, namely,*

$$A_1(x)E = EA_2(x)$$

for all $x \in \mathfrak{G}$.

If $R = k$ is a field then

$$\dim_k H_0(\mathfrak{G}\,;\, A_1, A_2) = I(A_1, A_2)$$

is called intertwinning number.

The "norm" of a matrix $T \in R_{r,s}$ defined by

$$\sum_{y \in \mathfrak{G}} A_1(y) T A_2(y^{-1})$$

is a 0-cocycle.

PROPOSITION 4. 2. *$H^1(\mathfrak{G}\ ;\ A_1, A_2)$ and matrix representations of type*

$$\begin{pmatrix} A_1(x) & E(x) \\ 0 & A_2(x) \end{pmatrix}$$

classified by

$$\begin{pmatrix} 1 & T \\ 0 & 1 \end{pmatrix}$$

are in one to one correspondences.

PROOF. From

$$\begin{pmatrix} A_1(x) & E(x) \\ 0 & A_2(x) \end{pmatrix}\begin{pmatrix} A_1(y) & E(y) \\ 0 & A_2(y) \end{pmatrix} = \begin{pmatrix} A_1(x)A_1(y) & A_1(x)E(y) + E(x)A_2(y) \\ 0 & A_2(x)A_2(y) \end{pmatrix}$$

it follows that this is a representation of $\mathfrak{G}$ if and only if

$$A_i(x)A_i(y) = A_i(xy) \qquad i = 1, 2$$
$$E(xy) = A_1(x)E(y) + E(x)A_2(y)$$

i. e. $E(x)$ is a 1-cocycle. The rest follows from direct computations. q. e. d.

Concerning the structure of R-module $H^n(\mathfrak{G}\ ;\ A_1, A_2)$ we have:

PROPOSITION 4. 3. *Let $g = \#\mathfrak{G}$ be the order of $\mathfrak{G}$. Then for any representations A_1, A_2,*

$$gH^n(\mathfrak{G}\ ;\ A_1, A_2) = 0, \qquad n > 0.$$

In particular if g is a unit in R,

$$H^n(\mathfrak{G}\ ;\ A_1, A_2) = 0, \qquad n > 0.$$

PROOF. Let $E(x_1, \ldots\ldots, x_n)$ be an n-cocycle, i. e.

$$\delta E(x_1, \ldots\ldots, x_{n+1}) = A_1(x_1)E(x_2, \ldots\ldots, x_{n+1}) + \sum_{i=1}^{n}(-1)^i E(x_1, \ldots\ldots, x_i x_{i+1}, \ldots\ldots, x_{n+1}) + (-1)^{n+1}E(x_1, \ldots\ldots, x_n)A_2(x_{n+1}).$$

Multiply $A_2(x_{n+1}^{-1})$ from right and add over $x_{n+1} \in \mathfrak{G}$ we have

$$A_1(x_1)\sum_{x\in\mathfrak{G}} E(x_2, \ldots\ldots, x_n, x)A_2(x^{-1}) + \sum_{i=1}^{n-1}(-1)\sum_{x\in\mathfrak{G}} E(x_1, \ldots\ldots, x_i x_{i+1}, \ldots\ldots x_n, x)E(x^{-1})$$

$$+(-1)^n \sum_{x\in\mathfrak{G}} E(x_1, \ldots\ldots, x_{n-1}, x_n x)A_2(x^{-1})$$
$$+(-1)^{n+1} gE(x_1, \ldots\ldots x_n) = 0.$$

If we put

$$F(x_1, \ldots\ldots, x_{n-1}) = \sum_{x\in\mathfrak{G}} E(x_1, \ldots\ldots, x_{n-1}, x)A_2(x^{-1})$$

in this equation, we have

$$gE(x_1, \ldots\ldots, x_n) = (-1)^n \; \delta F(x_1, \ldots\ldots x_n).$$

q. e. d.

PROPOSITION 4. 4. *If R is noetherian and R/gR is a finite ring, then*

$$\# H^n(\mathfrak{G}\,; A_1, A_2) < +\infty, \qquad n > 0.$$

PROOF. The R-module of n-cochains $C^n(\mathfrak{G}; A_1, A_2)$ is a finite R-module. Since R is noetherian, its submodule of n-cocycles $Z^n(\mathfrak{G}\,; A_1, A_2)$ is also a finite R-module, hence a priori $H^n(\mathfrak{G}; A_1, A_2)$ is a finite R-module. Since by Prop. 4. 3 any element $\mathbf{E} \in H^n(\mathfrak{G}; A_1, A_2)$ has finite order $g\ \mathbf{E} = 0$. This with the hypothesis $\# (R/gR) < +\infty$ implies

$$\# H^n(\mathfrak{G}; A_1, A_2) < +\infty.$$

5. Maschke pair. We say that two representations $A_1(x), A_2(x)$ of the group $\mathfrak{G}$ in matrices with elements in a commutative ring R with unity element form a Maschke pair if

$$H^1(\mathfrak{G}\,; A_1, A_2) = H^1(\mathfrak{G}\,; A_2, A_1) = 0,$$

By Prop. 4. 3. if p is a prime which does not divide the order g of $\mathfrak{G}$:

$$g \not\equiv 0\,(p)$$

and R is a field of characteristic p or $R = \mathfrak{o}_{\mathfrak{p}}$ a ring of $\mathfrak{p}$-adic integers with $\mathfrak{p}|p$, any two representations in R are Maschke pair.

Another example is:

PROPOSITION 5. 1. *Let $\Gamma = R[\mathfrak{G}]$ be the group ring of $\mathfrak{G}$ with coefficients in R. Assume that either representation module of A_1 be Γ-injective*[4] *or that of A_2 be Γ-projective*[4], *then*

$$H^1(\mathfrak{G}; A_1, A_2) = 0.$$

Notice that if a representation $A(x)$ is a direct constituent of the regular representation then its representation module is Γ-projective.

4) These terminologies are those used in Cartan-Eilenberg's "Homological Algebra".

PROOF. We prove only in case that the representation module A_2 of the representation $A_2(x)$ is Γ-projective, since other case is similar.

By Prop. 4.2 to any element $\mathbf{E} \in H^1(\mathfrak{G}; A_1, A_2)$ there corresponds an R-free Γ-module B such that

$$0 \to A_1 \to B \to A_2 \to 0$$

is exact. By Γ-projectivity of A_2 there exists a Γ-homomorphism

$$\varphi: A_2 \to B$$

such that

$$A_2 \to B \to A_2$$

is the identity map.

Let a basis of B be so chosen that

$$x(a_1, \ldots\ldots, a_r, b_1, \ldots\ldots, b_s) = (a_1, \ldots\ldots, a_r, b_1, \ldots\ldots, b_s) \begin{pmatrix} A_1(x) & E(x) \\ 0 & A_2(x) \end{pmatrix}$$

with $E(x) \in \mathbf{E}$. Since $(a_1, \ldots\ldots, a_r, \varphi(b_1), \ldots\ldots, \varphi(b_s))$ is a basis of B, there exist two matrices S, T with regular S such that

$$(a_1, \ldots\ldots, a_r, \varphi(b_1), \ldots\ldots, \varphi(b_s)) = (a_1, \ldots\ldots, a_r, b_1, \ldots\ldots, b_s) \begin{pmatrix} 1 & T \\ 0 & S \end{pmatrix}.$$

Put

$$(a_1, \ldots\ldots, a_r, b_1, \ldots\ldots, b_s) \begin{pmatrix} 1 & T \\ 0 & 1 \end{pmatrix} = (a_1, \ldots\ldots, a_r, c_1, \ldots\ldots, c_s).$$

Then $(a_1, \ldots\ldots, a_r, c_1, \ldots\ldots, c_s)$ is a basis of B such that

$$x(a_1, \ldots\ldots, a_r, c_1, \ldots\ldots, c_s) = (a_1, \ldots\ldots, a_r, c_1, \ldots\ldots, c_s) \begin{pmatrix} A_1(x) & 0 \\ 0 & A_2(x) \end{pmatrix}$$

By Prop. 4.2 this means $\mathbf{E} = 0$. q. e. d.

6. Representations in $\mathfrak{p}$-adic fields. In this section, $\mathfrak{p}$ is a finite prime in an algebraic number field k, $\mathfrak{o}_\mathfrak{p}$ the ring of $\mathfrak{p}$-adic integers.

THEOREM 1 (HENSEL LEMMA). *Let $A(x)$ be a representation of the group $\mathfrak{G}$ in matrices with elements in $\mathfrak{o}_\mathfrak{p}$. $\bar{A}(x)$ be the reduction mod $\mathfrak{p}$ of the representation $A(x)$. Assume in the modular field $\mathfrak{k}_\mathfrak{p} = \mathfrak{o}_\mathfrak{p}/\mathfrak{p}$ a direct decomposition* :

$$\bar{A}(x) \sim \begin{pmatrix} \mathfrak{A}_1(x) & 0 \\ 0 & \mathfrak{A}_2(x) \end{pmatrix}$$

in which $\mathfrak{A}_1$, $\mathfrak{A}_2$ *form a Maschke pair* (§5) *i.e.*

$$H^1(\mathfrak{G}\,;\mathfrak{A}_1,\mathfrak{A}_2)=H^1(\mathfrak{G}\,;\mathfrak{A}_2,\mathfrak{A}_1)=0.$$

Then there exists a direct decomposition in $\mathfrak{o}_\mathfrak{p}$:

$$A(x)\sim\begin{pmatrix} A_1(x) & 0 \\ 0 & A_2(x)\end{pmatrix}$$

such that

$$\bar{A}_i(x)=\mathfrak{R}_i(x) \qquad i=1,2.$$

PROOF. Without loss of generality, we may assume

$$\bar{A}(x)=\begin{pmatrix} \mathfrak{A}_1(x) & 0 \\ 0 & \mathfrak{A}_2(x)\end{pmatrix}.$$

Then the representation $A(x)$ has in $\mathfrak{o}_\mathfrak{p}$ the following form

$$A(x)=\begin{pmatrix} A_{11}(x) & \pi A_{12}(x) \\ \pi A_{21}(x) & A_{22}(x)\end{pmatrix}$$

where π is a primitive element for the prime $\mathfrak{p}$, and $A_{ij}(x)$ are matrices with elements in $\mathfrak{o}_\mathfrak{p}$. We prove by induction that representation of the form:

$$\begin{pmatrix} A_{11}(x) & \pi^n A_{12}(x) \\ \pi^m A_{21}(x) & A_{22}(x)\end{pmatrix}, \qquad n>0,\ m>0$$

with $A_{ij}(x)$ matrices in $\mathfrak{o}_\mathfrak{p}$, can be transformed by a matrix of type:

$$\begin{pmatrix} 1 & \pi^n T \\ 0 & 1\end{pmatrix}, \qquad T \text{ in } \mathfrak{o}_\mathfrak{p}$$

into the form

$$\begin{pmatrix} A'_{11}(x) & \pi^{n+1} A'_{12}(x) \\ \pi^m A'_{21}(x) & A'_{22}(x)\end{pmatrix}$$

with matrices $A'_{ij}(x)$ in $\mathfrak{o}_\mathfrak{p}$ such that

$$A_{ij}(x)\equiv A'_{ij}(x) \quad (\mathfrak{p}^{n+m}) \qquad i=1,2$$

under the condition

$$H^1(\mathfrak{G}\,;\mathfrak{A}_1,\ \mathfrak{A}_2)=0.$$

Similar result holds for m.
For, from

$$\begin{pmatrix} A_{11}(x) & \pi^n A_{12}(x) \\ \pi^m A_{21}(x) & A_{22}(x)\end{pmatrix}\begin{pmatrix} 1 & \pi^n T \\ 0 & 1\end{pmatrix}$$
$$=\begin{pmatrix} A_{11}(x) & \pi^n A_{11}(x)T+\pi^n A_{12}(x) \\ \pi^m A_{21}(x) & \pi^{n+m} A_{21}(x)T+A_{22}(x)\end{pmatrix}$$

$$\begin{pmatrix} 1 & \pi^n T \\ 0 & 1 \end{pmatrix}\begin{pmatrix} A'_{11}(x) & \pi^{n+1}A'_{12}(x) \\ \pi^m A'_{21}(x) & A'_{22}(x) \end{pmatrix}$$
$$= \begin{pmatrix} A'_{11}(x) + \pi^{n+m}TA'_{21}(x) & \pi^{n+1}A'_{12}(x) + \pi^n TA'_{22}(x) \\ \pi^m A'_{21}(x) & A'_{22}(x) \end{pmatrix}$$

the condition for the matrix T is

$$A_{11}(x)T + A_{12}(x) \equiv TA'_{12}(x) \qquad (\mathfrak{p}).$$

Since $\overline{A}_{12}(x) \in Z'(\mathfrak{G}; \mathfrak{A}_1, \mathfrak{A}_2)$ is a 1-cocycle, by hypothesis on $\mathfrak{A}_1, \mathfrak{A}_2$ such matrix T must exist in $\mathfrak{o}_\mathfrak{p}$.

Starting from

$$A(x) = \begin{pmatrix} A_{11}(x) & \pi A_{12}(x) \\ \pi A_{21}(x) & A_{22}(x) \end{pmatrix}$$

with $n = m = 1$ we arrive at the $\mathfrak{o}_\mathfrak{p}$-equivalence

$$A(x) \sim \begin{pmatrix} A_1(x) & 0 \\ 0 & A_2(x) \end{pmatrix}$$

with $\overline{A}_i(x) = \mathfrak{a}_i(x)$ $i = 1, 2$. q. e. d.

COROLLARY[5]. *Let $\mathfrak{U}$ be a directly indecomposable modular representation of the group $\mathfrak{G}$ contained in the regular representation. Then there exists a representation U in $\mathfrak{o}_\mathfrak{p}$ such that*

$$\overline{U}(x) = \mathfrak{U}(x).$$

For, in the modular field $\mathfrak{k}_\mathfrak{p}$, the regular representation $R(x)$ in $\mathfrak{o}_\mathfrak{p}$ splits as

$$\overline{R}(x) \sim \begin{pmatrix} \mathfrak{U} & 0 \\ 0 & \mathfrak{B} \end{pmatrix}$$

with suitable modular representation $\mathfrak{B}$. Thereby $\mathfrak{U}$, $\mathfrak{B}$ are represented by Γ-projective modules therefore form a Maschke pair.

THEOREM 2. *Let the prime $\mathfrak{p}$ does not divide order g of $\mathfrak{G}$. Then matrix representation $A(x)$ in $\mathfrak{o}_\mathfrak{p}$ and $\mathfrak{A}(x)$ in modular field $\mathfrak{k}_\mathfrak{p} = \mathfrak{o}_\mathfrak{p}/\mathfrak{p}$ are in one to one correspondences by reduction mod $\mathfrak{p}$:*

$$A(x) \rightarrow \overline{A}(x) = \mathfrak{A}(x).$$

In other words any representation in $\mathfrak{o}_\mathfrak{p}$ is completely reducible and there are as many irreducible representations in $\mathfrak{o}_\mathfrak{p}$ as that in $\mathfrak{k}_\mathfrak{p}$.

PROOF. Complete reducibility follows from Prop. 4. 3. If $A(x)$ is an irreducible representation in $\mathfrak{o}_\mathfrak{p}$ then its reduction mod $\mathfrak{p}$: $\overline{A}(x)$ is also ir-

5) This result was announced by Brauer [3].

reducible.

For, suppose contrary to our assertion

$$\overline{A}(x) \sim \begin{pmatrix} \mathfrak{A}_1(x) & 0 \\ 0 & \mathfrak{A}_2(x) \end{pmatrix}$$

then Hensel lemma would yield a decomposition

$$A(x) \sim \begin{pmatrix} A_1(x) & 0 \\ 0 & A_2(x) \end{pmatrix}$$

in $\mathfrak{o}_\mathfrak{p}$. This is a contradiction.

Conversely, assume $\mathfrak{A}(x)$ be an irreducible representation in $\mathfrak{k}_\mathfrak{p}$, then the regular representation $\mathfrak{R}(x)$ splits as

$$\mathfrak{R}(x) \sim \begin{pmatrix} \mathfrak{A}(x) & 0 \\ 0 & \mathfrak{B}(x) \end{pmatrix}.$$

Apply Hensel lemma to the regular representation $R(x)$ in $\mathfrak{o}_\mathfrak{p}$ with $\overline{R}(x) = \mathfrak{R}(x)$ we have

$$R(x) \sim \begin{pmatrix} A(x) & 0 \\ 0 & B(x) \end{pmatrix}$$

with $\overline{A}(x) = \mathfrak{A}(x)$. Of course $A(x)$ is irreducible in $\mathfrak{o}_\mathfrak{p}$. q. e. d.

COROLLARY. *In case* $g \not\equiv 0$ $(\mathfrak{p})$. *If two matrix representations* $A_1(x)$, $A_2(x)$ *are* $k_\mathfrak{p}$*-equivalent then they are* $\mathfrak{o}_\mathfrak{p}$*-equivalent.*

PROOF. Since $k_\mathfrak{p}$ is a field, ordinary theory of representations shows that

$$A_1(x) \sim \begin{pmatrix} B_1(x) & & 0 \\ & \ddots & \\ 0 & & B_s(x) \end{pmatrix} \sim A_2(x) \quad \text{in } k_\mathfrak{p},$$

where $B_1(x), \ldots\ldots, B_s(x)$ are irreducible representations in $k_\mathfrak{p}$. Since $\mathfrak{o}_\mathfrak{p}$ is a principal ideal domain, we may assume without loss of generality that $B_1(x), \ldots\ldots, B_s(x)$ are matrices with elements in $\mathfrak{o}_\mathfrak{p}$. From the Theorem 2

$$A_1(x) \sim \begin{pmatrix} C_1(x) & & 0 \\ & \ddots & \\ 0 & & C_t(x) \end{pmatrix} \quad \text{in } \mathfrak{o}_\mathfrak{p}$$

where $C_1, \ldots\ldots\ldots, C_t$ are irreducible representations in $\mathfrak{o}_\mathfrak{p}$. Comparing their characters, we see that $C_1, \ldots\ldots, C_t$ are permutations of $B_1, \ldots\ldots, B_s$ (By suitable $\mathfrak{o}_\mathfrak{p}$-transforms if necessary). The same is true for the representation $A_2(x)$. Therefore

$$A_1(x) \sim \begin{pmatrix} B_1(x) & & 0 \\ & \ddots & \\ 0 & & B_s(x) \end{pmatrix} \sim A_2(x) \quad \text{in } \mathfrak{o}_\mathfrak{p}$$

q. e. d.

Thus, the case $\mathfrak{p}$ with $g \not\equiv 0(\mathfrak{p})$ are completely studied. We are therefore in a position to investigate the case $g \equiv 0(\mathfrak{p})$. More precisely take integer $e_0 > 0$ such that

$$g \equiv 0 \ (\mathfrak{p}^{e_0})$$
$$g \not\equiv 0 \ (\mathfrak{p}^{e_0+1}).$$

PROPOSITION 6. 1 (PRINCIPAL GENUS THEOREM[6]). *Assume* $e \geqq e_0$ *and* $A_1(x)$, $A_2(x)$ *are representations in* $\mathfrak{o}_\mathfrak{p}$. *If an* n*-cocycle* $E \in Z^n(\mathfrak{G} ; A_1, A_2)$ *satisfies*

$$E(x_1, \ldots\ldots, x_n) \equiv 0 \ (\mathfrak{p}^e)$$

then there exists an $(n-1)$*-cochain* $F \in C^{n-1}(\mathfrak{G} ; A_1, A_2)$ *such that*

$$E = \delta F$$

with

$$F(x_1, \ldots\ldots, x_{n-1}) \equiv 0 \ (\mathfrak{p}^{e-e_0}).$$

PROOF. Since E is an n-cocycle, by the proof of Prop. 4. 3, if we put

$$F_1(x_1, \ldots\ldots, x_{n-1}) = \sum_{x \in \mathfrak{G}} E(x_1, \ldots\ldots, x_{n-1}, x) \ A_2(x^{-1})$$

then

$$gE = (-1)^n \delta F_1.$$

From the hypothesis $E \equiv 0 \, (\mathfrak{p}^e)$ it follows that

$$F = (-1)^n \frac{1}{g} F_1$$

is indeed an $(n-1)$-cochain in $\mathfrak{o}_\mathfrak{p}$ satisfying

$$F(x_1, \ldots\ldots, x_{n-1}) \equiv 0 \, (\mathfrak{p}^{e-e_0})$$
$$E = \delta F \qquad \text{q. e. d.}$$

PROPOSITION 6. 2. *Let* A_1, A_2 *be two representations in* $\mathfrak{o}_\mathfrak{p}$, *and* $e > e_0$ *be an integer. Then equivalences*:

$$A_1 \sim A_2 \qquad \textit{in } \mathfrak{o}_\mathfrak{p}/\mathfrak{p}^e$$

and

$$A_1 \sim A_2 \qquad \textit{in } \mathfrak{o}_\mathfrak{p}$$

are completely equivalent.

PROOF. Equivalence in $\mathfrak{o}_\mathfrak{p}$ implies equivalence in $\mathfrak{o}_\mathfrak{p}/\mathfrak{p}^e$ is trivial. Let us show the converse. Assume

$$A_1 \sim A_2 \qquad \text{in } \mathfrak{o}_\mathfrak{p}/\mathfrak{p}^e.$$

6) This proposition has some analogy to a result of Kuniyoshi-Takahashi [14].

In other words there exists a matrix T in $\mathfrak{o}_{\mathfrak{p}}$ such that

$$A_1T - TA_2 \equiv 0\,(\mathfrak{p}^e), \qquad \det\ T \not\equiv 0\,(\mathfrak{p}).$$

Then

$$E(x) = A_1(x)T - TA_2(x)$$

is a 1-cocycle $\in Z^1(\mathfrak{G};\ A_1,\ A_2)$ and

$$E(x) \equiv 0\ (\mathfrak{p}^e).$$

Since $e > e_0$, we can apply principal genus theorem (Prop. 6. 1) and it yields a matrix S in $\mathfrak{o}$ such that

$$E(x) = A_1(x)S - SA_2(x)$$
$$S \equiv 0\ (\mathfrak{p}^{e-e_0}).$$

If we put $T' = T - S$, then T' is a matrix in $\mathfrak{o}_{\mathfrak{p}}$ such that

$$A_1(x)T' = T'A_2(x)$$
$$\det\ T' \equiv \det\ T \not\equiv 0\ (\mathfrak{p})$$

i. e. $A_1(x), A_2(x)$ are $\mathfrak{o}_{\mathfrak{p}}$-equivalent. q. e. d.

7. Equivalence theory of Γ-lattices. In this section we use same notations as that of §2. Namely k is an algebraic number field and $\mathfrak{o}$ the ring of integers in k. $\Gamma = \mathfrak{o}[\mathfrak{G}]$ is the group ring over $\mathfrak{o}$.

PROPOSITION 7. 1. *There exists at least one* Γ-*lattice* M *in* V, *if* V *is a* Γ-*space.*

PROOF. If V is written by a k-basis as

$$V = v_1k + \cdots\cdots + v_mk,$$

then the following finite $\mathfrak{o}$-module

$$M = \sum_{x \in \mathfrak{G}} \sum_{i=1}^{m} xv_i\mathfrak{o}$$

is a Γ-lattice in V. q. e. d.

If $R \supseteq \mathfrak{o}$ is a ring over $\mathfrak{o}$, we put for a Γ-lattice M;

$\{M;\ R/\mathfrak{o}\} = \{N \in \Gamma\text{-lattices in } V \mid NR \simeq MR \text{ as } \Gamma R\text{-modules}\}$.

In particular

$$\{M\ ;\ k/\mathfrak{o}\}$$

is the set of all Γ-lattices in V, for any Γ-lattice M in V.

Since $M_1,\ M_2 \in \{M;\ R/\mathfrak{o}\}$ lie in the same class $\{M;\ k/\mathfrak{o}\}$, we can write

$$\{M;\ k/\mathfrak{o}\} = \{M_1;\ R/\mathfrak{o}\} + \cdots\cdots + \{M_c;\ R/\mathfrak{o}\}$$

as a disjoint union of finite or infinite number of subclasses. We put

$$c = c(R/\mathfrak{o})$$

and call it the class number of Γ-lattices with respect to R.

If K/k is an extension field with a maximal order $\mathfrak{O} \supseteq \mathfrak{o}$, we can define $\Gamma\mathfrak{O}$-lattices in VK and the symbol

$$\{M;\ R/\mathfrak{O}\}$$

with a ring $R \supseteq \mathfrak{P}$. There exists always a map

$$\{M; R/\mathfrak{o}\} \ni M_1 \to M_1\mathfrak{O} \in \{M; R/\mathfrak{O}\}$$

called injection.

Main examples of R and $\mathfrak{O}$ are:

$K = k_{\mathfrak{p}}$: $\mathfrak{p}$-adic completion of the field k, $\mathfrak{O} = \mathfrak{o}_{\mathfrak{p}}$: $\mathfrak{p}$-adic integers in $k_{\mathfrak{p}}$,

$R = \mathfrak{o}(\mathfrak{p}_1, \ldots\ldots, \mathfrak{p}_r) = \bigcap_{i=1}^{r}(k \cap \mathfrak{o}_{\mathfrak{p}_i}) \supseteq \mathfrak{o}$ where $\mathfrak{p}_1, \ldots\ldots, \mathfrak{p}_r$ are finite primes in k.

PROPOSITION 7.2.[7] *The injection*

$$\{M;\ k/\mathfrak{o}\} \to \{M\mathfrak{o}_{\mathfrak{p}};\ k_{\mathfrak{p}}/\mathfrak{o}_{\mathfrak{p}}\}$$

is an onto map with same class number

$$c(\mathfrak{o}_{\mathfrak{p}}/\mathfrak{o}) = c(\mathfrak{o}_{\mathfrak{p}}/\mathfrak{o}_{\mathfrak{p}}).$$

PROOF. Take an $M^{(\mathfrak{p})} \in \{M\mathfrak{o}_{\mathfrak{p}}; k_{\mathfrak{p}}/\mathfrak{o}_{\mathfrak{p}}\}$, we can define a Γ-lattice $M_1 \in \{M; k/\mathfrak{o}\}$ such that $M_1\mathfrak{o}_{\mathfrak{p}} = M^{(\mathfrak{p})}$. Namely, let M be a Γ-lattice in V. Put

$$M_1^{(\mathfrak{p})} = M^{(\mathfrak{p})}$$
$$M_1^{(\mathfrak{q})} = M\mathfrak{o}_{\mathfrak{q}} \qquad \text{for prime } \mathfrak{q} \neq \mathfrak{p}.$$

Then

$$M_1 = \bigcap_{\mathfrak{q}}(M_1^{(\mathfrak{q})} \cap V)$$

is a desired Γ-lattice with $M_1\mathfrak{o}_{\mathfrak{p}} = M^{(\mathfrak{p})}$ by Prop. 1.3.
As to class numbers $c(\mathfrak{o}_{\mathfrak{p}}/\mathfrak{o})$, $c(\mathfrak{o}_{\mathfrak{p}}/\mathfrak{o}_{\mathfrak{p}})$,

$$M_1,\ M_2 \in \{M_3;\ \mathfrak{o}_{\mathfrak{p}}/\mathfrak{o}\}$$

imply $M_1\mathfrak{o}_{\mathfrak{p}} \simeq M_2\mathfrak{o}_{\mathfrak{p}}$ as $\Gamma\mathfrak{o}_{\mathfrak{p}}$-modules.
Therefore

$$M_1\mathfrak{o}_{\mathfrak{p}},\ M_2\mathfrak{o}_{\mathfrak{p}} \in \{M_3\mathfrak{o}_{\mathfrak{p}},\ \mathfrak{o}_{\mathfrak{p}}/\mathfrak{o}_{\mathfrak{p}}\}$$

and conversely. q. e. d.

PROPOSITION 7.3. *For any Γ-lattice M*

$$\{M; \mathfrak{o}(\mathfrak{p})/\mathfrak{o}\} = \{M; \mathfrak{o}_{\mathfrak{p}}/\mathfrak{o}\}.$$

PROOF. Since $M_1\mathfrak{o}(\mathfrak{p}) \simeq M_2\mathfrak{o}(\mathfrak{p})$ as $\Gamma\mathfrak{o}(\mathfrak{p})$-modules implies $M_1\mathfrak{o}_{\mathfrak{p}} \simeq M_2\mathfrak{o}_{\mathfrak{p}}$ as

7) This and following Prop. 7.3 give a proof for locality of Maranda [16]' s concepts of $\mathfrak{p}$-equivalence and genus, noticed in the introduction.

$\Gamma\mathfrak{o}_\mathfrak{p}$-modules, it ts trivial that

$$\{M;\ \mathfrak{o}(\mathfrak{p})/\mathfrak{o}\} \subseteq \{M;\ \mathfrak{o}_\mathfrak{p}/\mathfrak{o}\}.$$

Conversely, suppose $M_1,\ M_2 \in \{M;\ \mathfrak{o}_\mathfrak{p}/\mathfrak{o}\}$.
Since $\mathfrak{o}(\mathfrak{p})$ is a principal ideal domain, we can write

$$M_1\mathfrak{o}(\mathfrak{p}) = u_1\mathfrak{o}(\mathfrak{p}) \oplus \cdots\cdots \oplus u_m\mathfrak{o}(\mathfrak{p})$$
$$M_2\mathfrak{o}(\mathfrak{p}) = v_1\mathfrak{o}(\mathfrak{p}) \oplus \cdots\cdots \oplus v_m\mathfrak{o}(\mathfrak{p})$$

with matrix representations with elements in $\mathfrak{o}(\mathfrak{p})$:

$$x\mathfrak{u} = \mathfrak{u}A_1(x)$$
$$x\mathfrak{v} = \mathfrak{v}A_2(x).$$

The $\Gamma\mathfrak{o}_\mathfrak{p}$-isomorphism $\varphi:\ M_2\mathfrak{o}_\mathfrak{p} \to M_1\mathfrak{o}_\mathfrak{p}$ can be written as

$$\varphi(\mathfrak{v}) = \mathfrak{u}\cdot T$$

with matrix T in $\mathfrak{o}_\mathfrak{p}$ such that $\det T \not\equiv 0\ (\mathfrak{p})$.
In terms of matrix representations $A_1(x)$, $A_2(x)$ we have

$$A_1(x)T = TA_2(x).$$

Take an exponent $e > e_0$ with $g = \#\mathfrak{G} \equiv 0\ (\mathfrak{p}^{e_0})$ but $g \not\equiv 0\ (\mathfrak{p}^{e_0+1})$, there exists a matrix T in $\mathfrak{o}$ such that

$$T_1 \equiv T\ (\mathfrak{p}^e).$$

Consider a 1-cocycle

$$E(x) = A_1(x)T_1 - T_1A_2(x) \equiv 0\ (\mathfrak{p}^e)$$

in $\mathfrak{o}(\mathfrak{p})$. By the principal genus theorem[8] (Prop. 6. 1) we can find a matrix S in $\mathfrak{o}(\mathfrak{p})$ such that

$$E(x) = A_1(x)S - SA_2(x)$$

with $S \equiv 0\ (\mathfrak{p}^{e-e_0})$ and hence $S \equiv 0\ (\mathfrak{p})$.
Then $T_2 = T_1 - S$ is a matrix in $\mathfrak{o}(\mathfrak{p})$ intertwines $A_1(x)$, $A_2(x)$:

$$A_1(x)T_2 = T_2A_2(x)$$

such that

$$\det T_2 \equiv \det T_1 \equiv \det T \not\equiv 0\ (\mathfrak{p}).$$

Therefore the new map

$$\psi(\mathfrak{v}) = \mathfrak{u}\ T_2$$

is a $\Gamma\mathfrak{o}(\mathfrak{p})$-isomorphism $M_1\mathfrak{o}(\mathfrak{p}) \simeq M_2\mathfrak{o}(\mathfrak{p})$ i. e.

$$M_1,\ M_2 \in \{M;\ \mathfrak{o}(\mathfrak{p})/\mathfrak{o}\}.$$ q. e. d.

PROPOSITION 7. 4. *If* $\mathfrak{p}_1, \cdots\cdots, \mathfrak{p}_r$ *are finite primes in* k,

8) This holds for the ring $\mathfrak{o}(\mathfrak{p})$ instead of $\mathfrak{o}_\mathfrak{p}$ if we consider its proof.

$$\{M;\mathfrak{o}(\mathfrak{p}_1,\ldots\ldots,\mathfrak{p}_r)/\mathfrak{o}\}=\bigcap_{i=1}^{r}\{M;\mathfrak{o}_{\mathfrak{p}_i}/\mathfrak{o}\}.$$

PROOF. From preceding Prop. 7.3 we have only to prove

$$\{M;\mathfrak{o}(\mathfrak{p}_1,\ldots\ldots,\mathfrak{p}_r)/\mathfrak{o}\}$$
$$=\bigcap_{i=1}^{r}\{M;\mathfrak{o}(\mathfrak{p}_i)/\mathfrak{o}\}.$$

Since $\mathfrak{o}(\mathfrak{p}_1,\ldots\ldots,\mathfrak{p}_r)\subseteq\mathfrak{o}(\mathfrak{p}_i)$, it is clear that

$$\{M;\mathfrak{o}(\mathfrak{p}_1,\ldots\ldots,\mathfrak{p}_r)/\mathfrak{o}\}\subseteq\bigcap_{i=1}^{r}\{M;\mathfrak{o}(\mathfrak{p}_i)/\mathfrak{o}\}.$$

Take an $M_1\in\bigcap_{i=1}^{r}\{M;\mathfrak{o}(\mathfrak{p}_i)/\mathfrak{o}\}$ and put

$$\mathfrak{o}'=\mathfrak{o}(\mathfrak{p}_1,\ldots\ldots,\mathfrak{p}_r).$$

Since $\mathfrak{o}'$ is a principal ideal domain, we can express the proposition, if we take suitable $\mathfrak{o}'$-basis of Γ-lattices in consideration, by words of matrix representations. Namely, if $A_1(x)$, $A_2(x)$ be two matrix representations in $\mathfrak{o}'$, such that there exist matrices T_i in $\mathfrak{o}(\mathfrak{p}_i)$ $(i=1,\ldots\ldots,r)$ with $\det T_i\not\equiv 0$ $(\mathfrak{p}_i)$ and

$$A_1(x)T_i=T_iA_2(x)\qquad i=1,\ldots\ldots,r,$$

we can find a matrix T in $\mathfrak{o}'$ with T^{-1} in $\mathfrak{o}'$ and

$$A_1(x)T=TA_2(x).$$

Take elements $\omega_i\in\mathfrak{o}'$ such that

$$\omega_i\not\equiv 0\,(\mathfrak{p}_i),\ \omega_i\equiv 0\,(\mathfrak{p}_j^{e_j})\qquad j\neq i,\ 1\leqq i,\ j\leqq r,$$

whose exponents $e_j>0$ are taken as

$$\pi_j^{e_j}T_i\equiv 0\ (\mathfrak{p}_j)$$

with primitive element π_j of $\mathfrak{p}_j$.
Then the matrix

$$T=\sum_{i=1}^{r}\omega_iT_i$$

is a desired matrix in $\mathfrak{o}'$. Since

$$\det T\equiv\det\omega_jT_j\equiv\omega_j^m\det T_j\not\equiv 0\,(\mathfrak{p}_j)$$
$$j=1,\ldots\ldots\ldots,r.$$

q. e. d.

PROPOSITION 7.5. *If a finite prime $\mathfrak{p}_r$ is different from $\mathfrak{p}_1,\ldots\ldots,\mathfrak{p}_{r-1}$, then*

$$\{M_1;\mathfrak{o}(\mathfrak{p}_1,\ldots\ldots,\mathfrak{p}_{r-1})/\mathfrak{o}\}\cap\{M_2;\mathfrak{o}(\mathfrak{p}_r)/\mathfrak{o}\}\neq\phi$$

for any Γ-*lattices* M_1, M_2 *in* V.

PROOF. Put $\mathfrak{o}' = \mathfrak{o}(\mathfrak{p}_1, \ \dots, \mathfrak{p}_r)$. This is a principal ideal domain and each ideal in $\mathfrak{o}'$ is of the form:

$$\left(\prod_{i=1}^{r} \pi_i^{e_i}\right)$$

with primitive elements π_i of $\mathfrak{p}_i$ with $\pi_j \not\equiv 0\,(\mathfrak{p}_j)$ for $i \neq j$. We can also prove the proposition by words of matrix representations. Since two matrix representations $A_1(x)$, $A_2(x)$ in $\mathfrak{o}'$ are k-equivalent, there exists a non-singular matrix T such that

$$A_1(x)T = TA_2(x)$$

with elements in $\mathfrak{o}$ if we multiply T by an element in $\mathfrak{o}$ if necessary.
By elementary divisor theory in $\mathfrak{o}'$ we can find "unimodular" matrices R, S in $\mathfrak{o}'$ such that

$$RTS = \begin{pmatrix} \prod_{i=1}^{r} \pi_i^{e_{i1}} & & 0 \\ & \ddots & \\ 0 & & \prod_{i=1}^{r} \pi_i^{e_{im}} \end{pmatrix}$$

with exponents

$$e_{i1} \leqq \cdots\cdots\cdots \leqq e_{im}, \qquad i = 1, \ldots\ldots\ldots, r.$$

Put $RTS = T_1T_2$ with

$$T_1 = \begin{pmatrix} \pi_r^{e_{r1}} & & 0 \\ & \ddots & \\ 0 & & \pi_r^{e_{rm}} \end{pmatrix}, \quad T_2 = \begin{pmatrix} \prod_{i=1}^{r-1} \pi_i^{e_{i1}} & & 0 \\ & \ddots & \\ 0 & & \prod_{i=1}^{r-1} \pi_i^{e_{im}} \end{pmatrix}$$

then these are matrices in $\mathfrak{o}'$ such that

$$\det T_1 \not\equiv 0\,(\mathfrak{p}_i) \qquad 1 \leqq i \leqq r-1; \ \det T_2 \not\equiv 0\,(\mathfrak{p}_r)$$

From the computations:

$$RA_1(x)R^{-1} \cdot RTS = RTS \cdot S^{-1}A_2(x)S$$

$$T_1^{-1}RA_1(x)R^{-1} \cdot T_1 = T_2S^{-1}A_2(x)S \cdot T_2^{-1} = A_2(x)$$

we see that $A_1(x)$ and $A_3(x)$ are $\mathfrak{o}(\mathfrak{p}_1, \ldots\ldots, \mathfrak{p}_{r-1})$-equivalent while $A_2(x)$ and $A_3(x)$ are $\mathfrak{o}(\mathfrak{p}_r)$-equivalent.
If we write M_3 for a Γ-lattice which represents $\mathfrak{G}$ by matrices $A_3(x)$, we have

$$M_3 \in \{M_1; \mathfrak{o}(\mathfrak{p}_1, \ldots\ldots, \mathfrak{p}_{r-1})\}$$

$$\cap \{M_2;\, \mathfrak{o}(\mathfrak{p}_r)\} \neq \phi. \qquad \text{q. e. d.}$$

THEOREM 3. *If $\mathfrak{p}_1, \ldots\ldots, \mathfrak{p}_r$ are mutually different finite primes in k, then we have for class numbers*:

$$c(\mathfrak{o}(\mathfrak{p}_1, \ldots\ldots, \mathfrak{p}_r)/\mathfrak{o}) = \prod_{i=1}^{r} c(\mathfrak{o}_{\mathfrak{p}_i}/\mathfrak{o}).$$

PROOF. It will be sufficient to prove

$$c(\mathfrak{o}(\mathfrak{p}_1, \ldots\ldots, \mathfrak{p}_r)/\mathfrak{o}) = \prod_{i=1}^{r} c(\mathfrak{o}(\mathfrak{p}_i)/\mathfrak{o}).$$

We prove this by induction on r. For $r = 1$ this is trivial. Let $r > 1$, we have by definition:

$$\begin{aligned}\{M;\, k/\mathfrak{o}\} &= \{M_1;\, \mathfrak{o}(\mathfrak{p}_1, \ldots\ldots, \mathfrak{p}_{r-1})/\mathfrak{o}\} \\ &\quad + \ldots\ldots + \{M_c;\, \mathfrak{o}(\mathfrak{p}_1, \ldots\ldots, \mathfrak{p}_{r-1})/\mathfrak{o}\} \\ &= \{N_1;\, \mathfrak{o}(\mathfrak{p}_r)/\mathfrak{o}\} + \ldots\ldots + \{N_d;\, \mathfrak{o}(\mathfrak{p}_r)/\mathfrak{o}\}, \\ &= \sum_{i,j} [\{M_i;\, \mathfrak{o}(\mathfrak{p}_1, \ldots\ldots, \mathfrak{p}_{r-1})/\mathfrak{o}\} \cap \{N_j;\, \mathfrak{o}(\mathfrak{p}_r)/\mathfrak{o}\}]\end{aligned}$$

with $c = c(\mathfrak{o}(\mathfrak{p}_1, \ldots\ldots, \mathfrak{p}_{r-1})/\mathfrak{o})$ and $d = c(\mathfrak{o}(\mathfrak{p}_r)/\mathfrak{o})$.
From the preceding Prop. 7.5 we have

$$\{M_i;\, \mathfrak{o}(\mathfrak{p}_1, \ldots\ldots, \mathfrak{p}_{r-1})/\mathfrak{o}\} \cap \{N_j;\, \mathfrak{o}(\mathfrak{p}_r)/\mathfrak{o}\} \neq \phi.$$

If we take a Γ-lattice M_{ij} in this intersection we have

$$\begin{aligned}&\{M_i;\, \mathfrak{o}(\mathfrak{p}_1, \ldots\ldots, \mathfrak{p}_{r-1})/\mathfrak{o}\} \cap \{N_j;\, \mathfrak{o}(\mathfrak{p}_r)/\mathfrak{o}\} \\ &\quad = \{M_{ij};\, \mathfrak{o}(\mathfrak{p}_1, \ldots\ldots, \mathfrak{p}_r)/\mathfrak{o}\}\end{aligned}$$

by Prop. 7.4.
Since

$$\{M;\, k/\mathfrak{o}\} = \sum_{i,j} \{M_{ij};\, \mathfrak{o}(\mathfrak{p}_1, \ldots\ldots \mathfrak{p}_r)/\mathfrak{o}\}$$

is disjoint, we have finally

$$c(\mathfrak{o}(\mathfrak{p}_1, \ldots\ldots, \mathfrak{p}_r)/\mathfrak{o}) = c(\mathfrak{o}(\mathfrak{p}_1, \ldots\ldots \mathfrak{p}_{r-1})/\mathfrak{o}) \cdot c(\mathfrak{o}(\mathfrak{p}_r)/\mathfrak{o}). \qquad \text{q. e. d.}$$

8. Genus of representations. Let $\tilde{k}$ be the adèle ring (or ring of valuation vectors) of k. $\tilde{\mathfrak{o}}$ denotes subring of $\tilde{k}$ consists of all integral elements of $\tilde{k}$ i. e. a direct sum

$$\tilde{\mathfrak{o}} = \sum_{\mathfrak{p}} \mathfrak{o}_{\mathfrak{p}}$$

of all $\mathfrak{p}$-adic integers $\mathfrak{o}_{\mathfrak{p}}$ for finite primes $\mathfrak{p}$ and $\mathfrak{o}_{\mathfrak{p}} = k_{\mathfrak{p}}$ for infinite primes

$\mathfrak{p} = \mathfrak{p}_\infty$.

As in the preceding §7, we define

$$\{M; \tilde{\mathfrak{o}}/\mathfrak{o}\}$$

and call Γ-lattices in them as belonging to the same genus. The class number $j = c\ (\tilde{\mathfrak{o}}/\mathfrak{o})$ defined by

$$\{M;\ k/\mathfrak{o}\} = \{M_1\ ;\ \tilde{\mathfrak{o}}/\mathfrak{o}\} + \ldots\ldots + \{M_j;\ \tilde{\mathfrak{o}}/\mathfrak{o}\}$$

is called the genus number of Γ-lattices in V.

THEOREM 4. *Let* $g = \#\mathfrak{G}$ *be the order of* $\mathfrak{G}$, *then for any* Γ*-lattice* M *in* V

$$\{M;\ \tilde{\mathfrak{o}}/\mathfrak{o}\} = \bigcap_{\mathfrak{p}|g} \{M;\ \mathfrak{o}_\mathfrak{p}/\mathfrak{o}\}.$$

From this we have

$$j = \prod_{\mathfrak{p}|g} c(\mathfrak{o}_\mathfrak{p}/\mathfrak{o}) < +\infty.$$

PROOF. M_1, $M_2 \in \{M;\ \tilde{\mathfrak{o}}/\mathfrak{o}\}$ imply by definition

$$M_1\tilde{\mathfrak{o}} \simeq M_2\tilde{\mathfrak{o}}$$

as $\Gamma\mathfrak{o}$-modules. Since $\tilde{\mathfrak{o}} = \sum_\mathfrak{p} \mathfrak{o}_\mathfrak{p}$ is a direct sum, we have for all primes $\mathfrak{p}$

$$M_1\mathfrak{o}_\mathfrak{p} \simeq M_2\mathfrak{o}_\mathfrak{p}$$

as $\Gamma\mathfrak{o}_\mathfrak{p}$-modules. Since this is trivially verified for infinite primes $\mathfrak{p} = \mathfrak{p}_\infty$, it is sufficient to prove that if $\mathfrak{p} \nmid g$

$$\{M;\ k/\mathfrak{o}\} = \{M;\ \mathfrak{o}_\mathfrak{p}/\mathfrak{o}\}.$$

But this follows at once from Coroll. to Theorem 2. The formula for j follows from

$$\{M;\ \tilde{\mathfrak{o}}/\mathfrak{o}\} = \bigcap_{\mathfrak{p}|g} \{M;\ \mathfrak{o}_\mathfrak{p}/\mathfrak{o}\} = \{M;\ \mathfrak{o}(\mathfrak{p}_1, \ldots\ldots, \mathfrak{p}_r)/\mathfrak{o}\}.$$

if we write $\mathfrak{p}_1, \ldots\ldots, \mathfrak{p}_r$ for all different primes dividing g.
Finally finiteness of $c(\mathfrak{o}_\mathfrak{p}/\mathfrak{o})$ follows from Prop. 6. 2. q. e. d.

9. Class number in a genus. Let V be a vector space over k, which has as in preceding sections $\mathfrak{G}$ as left operators and induces a representation

$$\mathfrak{G} \ni x \to A(x) \in GL(V;\ k)$$

by automorphism of V.

Similarly, for any prime $\mathfrak{p}$, the $\mathfrak{p}$-extension $V_\mathfrak{p} = Vk_\mathfrak{p}$ induces a representation which we write by the same symbol

$$A(x) \in GL(V_\mathfrak{p};\ k_\mathfrak{p}).$$

Moreover, the vector space $\widetilde{V} = V\widetilde{k}$ over adèle ring $\widetilde{k}$ of k induces a representation which will be also written by

$$A(x) \in GL(\widetilde{V}; \widetilde{k}).$$

There group $GL(\widetilde{V}; \widetilde{k})$ consists of elements

$$\widetilde{S} = (S_{\mathfrak{p}}),\ S_{\mathfrak{p}} \in GL(V_{\mathfrak{p}}; k_{\mathfrak{p}})$$

such that except for a finite set of primes, $S_{\mathfrak{p}}$ being $\mathfrak{p}$-unimodular.
Now,

$$G = v(A(\mathfrak{G})) = \{S \in GL(V; k) \mid A(x)S = SA(x) \text{ for all } x \in \mathfrak{G}\}$$

is an algebraic group of automorphisms of V. Its idèle group[9] is given by

$$\widetilde{G} = \widetilde{v}(A(\mathfrak{G})) = \{\widetilde{S} \in GL(\widetilde{V}; \widetilde{k}) \mid A(x)\widetilde{S} = \widetilde{S}A(x) \text{ for all } x \in \mathfrak{G}\}.$$

$\widetilde{G}$ contains G as a discrete subgroup with its natural topology.

Let M be a lattice in V. We define $M \cdot \widetilde{S}$ with $\widetilde{S} \in GL(\widetilde{V}; \widetilde{k})$ by

$$M \cdot \widetilde{S} = \bigcap_{\mathfrak{p}} (V \cap M_{\mathfrak{p}} S_{\mathfrak{p}}) \text{ if } \widetilde{S} = (S_{\mathfrak{p}}).$$

It is readly seen that $M \cdot \widetilde{S}$ is a lattice. Moreover if M is a Γ-lattice and $\widetilde{S} \in \widetilde{G}$ then $M \cdot \widetilde{S}$ is also a Γ-lattice.

PROPOSITION 9. 1. *Let M be a Γ-lattice in V, then*

$$\{M; \widetilde{\mathfrak{o}}/\mathfrak{o}\} = \{M \cdot \widetilde{S} \mid \widetilde{S} \in \widetilde{G}\}.$$

PROOF. "The fact that $M \cdot \widetilde{S}$ is a also a Γ-attice" is already remarked. $M \cdot \widetilde{S}$ is contained in $\{M; \widetilde{\mathfrak{o}}/\mathfrak{o}\}$. For if we fix a prime $\mathfrak{p}$, then

$$(M\widetilde{S})_{\mathfrak{p}} = M_{\mathfrak{p}} S_{\mathfrak{p}}$$

$$\varphi_{\mathfrak{p}};\ M_{\mathfrak{p}} \rightarrow M_{\mathfrak{p}} S_{\mathfrak{p}}$$

is a $\Gamma\mathfrak{o}_{\mathfrak{p}}$-isomorphism by virtue of

$$A(x)S_{\mathfrak{p}} = S_{\mathfrak{p}} A(x)$$

for all $x \in \mathfrak{G}$.

Conversely, take an $M_1 \in \{M; \widetilde{\mathfrak{o}}/\mathfrak{o}\}$ arbitrarily. For any prime $\mathfrak{p}$, we have by definition:

$$M_{1\mathfrak{p}} \simeq M_{\mathfrak{p}} \text{ as } \Gamma\mathfrak{o}_{\mathfrak{p}}\text{-modules}.$$

Since these are $\mathfrak{o}_{\mathfrak{p}}$-free modules, we can find $S_{\mathfrak{p}} \in GL(V_{\mathfrak{p}}; k)$ such that

$$M_{1\mathfrak{p}} = M_{\mathfrak{p}} S_{\mathfrak{p}}.$$

From the fact that M, M_1 are lattices in V it follows that $S_{\mathfrak{p}}$ are $\mathfrak{p}$-unimodu-

9) Idèle group of an algebraic group was considered by Ono [17], Tamagawa and Weil.

lar except for a finite number of primes, i. e.

$$\widetilde{S} = (S_\mathfrak{p}) \in GL(\widetilde{V}; \widetilde{k}).$$

Now, for any prime $\mathfrak{p}$ we have

$$xM_{1\mathfrak{p}} = M_{1\mathfrak{p}}A(x)$$
$$xM_\mathfrak{p} = M_\mathfrak{p}A(x)$$

hence $A(x)S_\mathfrak{p} = S_\mathfrak{p}A(x)$. This shows that $\widetilde{S} \in \widetilde{G}$ and

$$M_1 = M \cdot \widetilde{S}.$$ q. e. d.

PROPOSITION 9. 2. *Let M be a Γ-lattice in V, then*

$$\{M; \mathfrak{o}/\mathfrak{o}\} = \{MS \mid S \in G\}.$$

PROOF. If $S \in G$, then the fact $M \to M \cdot S$ is a Γ-isomorphism is trivial. Take an $M_1 \in \{M; \mathfrak{o}/\mathfrak{o}\}$ arbitrarily, there exists a Γ-isomorphism

$$\varphi : M \to M_1.$$

Since lattices in V generate V over k and are regular $\mathfrak{o}$-modules, we can generate V extend φ uniquely to a Γk-isomorphism[10)]

$$\varphi : Mk = V \to M_1k = V.$$

Therefore there exists $S \in GL(V; k)$ such that

$$M_1 = MS.$$

Finally Γ-isomorphism of φ implies $S \in G$. q. e. d

THEOREM 5. *Let M be a Γ-lattice in V. Put*

$$\widetilde{U} = \{\widetilde{T} \in \widetilde{G} \mid M\widetilde{T} = M\}$$

for a subgroup which fixes M. Then classes in a genus

$$\{M; \widetilde{\mathfrak{o}/\mathfrak{o}}\} = \{M_1; \mathfrak{o}/\mathfrak{o}\} + \ldots\ldots + \{M_c; \mathfrak{o}/\mathfrak{o}\}$$

are in one to one correspondences with double cosets

$$\widetilde{U}\backslash G/\widetilde{G}$$

of $\widetilde{G}$ with respect to two subgroups $\widetilde{U}$ and G. Explicitly, its correspondences are given by

$$\widetilde{G} \ni \widetilde{S} \to M \cdot \widetilde{S} \in \{M; \widetilde{\mathfrak{o}/\mathfrak{o}}\}$$
$$M\widetilde{S}_1 \simeq M\widetilde{S}_2 \text{ as } \Gamma\text{-lattices,}$$

if and only if

$$\widetilde{S}_1 = \widetilde{T}\widetilde{S}_2 \cdot S$$

with suitable $\widetilde{T} \in \widetilde{U}$, $S \in G$.

10) The proof is straightforward e. g. Chevalley [6].

PROOF. That the mapping

$$\tilde{G} \ni \tilde{S} \to M\tilde{S} \in \{M; \tilde{\mathfrak{o}}/\mathfrak{o}\}$$

is onto was already given by Prop. 9.1.
From

$$M\tilde{S}_1 \simeq M\tilde{S}_2 \text{ as } \Gamma\text{-lattices,}$$

we can find by Prop. 9.2 and $S \in G$ such that

$$M\tilde{S}_1 = M\tilde{S}_2 \cdot S.$$

This finally means an existence of $\tilde{T} \in \tilde{U}$ with

$$\tilde{S}_1 = \tilde{T} \cdot \tilde{S}_2 \cdot S \qquad \text{q. e. d.}$$

Notice that in a recent paper by Ono [17] it was proved that the number of double cosets $\# \tilde{U}\backslash\tilde{G}/G$ is always finite if G is a commutative algebraic group.

10. Absolutely irreducible representations. In the preceding §9, we have seen that class number in a genus is expressible as the number of double cosets

$$\tilde{U} \backslash \tilde{G} / G$$

of a suitable algebraic group G of automorphisms.

In this and following sections we shall consider more closely this double cosets.

PROPOSITION 10.1. *If M is a lattice in V, then the ring*

$$R = \{\alpha \in k \mid M\alpha \subseteq M\}$$

coincides with $\mathfrak{o}$.

PROOF. Since M is an $\mathfrak{o}$-module, $M\mathfrak{o} \subseteq M$, therefore

$$R \supseteq \mathfrak{o}.$$

Take an $\alpha \in k$ such that $M\alpha \subseteq M$. We have to show for any finite prime $\mathfrak{p}$ that

$$\alpha \in \mathfrak{o}_\mathfrak{p}.$$

Since $\mathfrak{o}_\mathfrak{p}$ is a principal ideal domain we can write

$$M_\mathfrak{p} = u_1\mathfrak{o}_\mathfrak{p} \oplus \cdots\cdots \oplus u_m\mathfrak{o}_\mathfrak{p}$$

as a direct sum. $M_\mathfrak{p}\alpha \subseteq M_\mathfrak{p}$ implies in particular

$$u_1\alpha = u_1\beta_1 + \cdots\cdots + u_m\beta_m$$

with $\beta_i \in \mathfrak{o}_\mathfrak{p}$. Take $\gamma \neq 0$, $\gamma \in \mathfrak{o}_\mathfrak{p}$ such that $\alpha\gamma \in \mathfrak{o}_\mathfrak{p}$, then

$$u_1\alpha\gamma = u_1\beta_1\gamma + \cdots\cdots + u_m\beta_m\gamma$$

hence we have

$$\alpha\gamma = \beta_1\gamma.$$

This implies $\alpha = \beta_1 \in \mathfrak{o}_\mathfrak{p}$. q. e. d.

THEOREM 6. *If V is an absolutely irreducible space and M is a Γ-lattice in V, then*

$$\tilde{G} = \tilde{\alpha} I \text{ with } \tilde{\alpha} \in J = J(k)$$
$$G = \alpha I \text{ wiih } \alpha \in k^\times$$
$$\tilde{U} = \tilde{\varepsilon} I \text{ with } \tilde{\varepsilon} \in U = U(k)$$

where, $J(k)$ is the group of idèles of k with principal idèles $k^\times$ and units idèles $U(k)$. Therefore

$\tilde{U} \backslash \tilde{G}/G \simeq$ *absolute ideal class group of k.*

PROOF. Since V is absolutely irreducible, so also is $V_\mathfrak{p}$ for any prime $\mathfrak{p}$. Therefore the structures of $\tilde{G}$ and G are as in the theorem. For the structure of

$$\tilde{U} = \tilde{\varepsilon} I, \ \tilde{\varepsilon} \in U(k)$$

we have to notice Prop 10. 1 or more precisely its proof, since by definition

$$\tilde{U} = \{\alpha I \mid \tilde{\alpha} \in J, \ M\tilde{\alpha} = M\}.$$ q. e. d.

COROLLARY. *If V is absolutely irreducible and M is a Γ-lattice in V, then the class number $c = c(\mathfrak{o}/\mathfrak{o})$:*

$$\{M; k/\mathfrak{o}\} = \{M_1; \mathfrak{o}/\mathfrak{o}\} + \dots\dots + \{M_c; \mathfrak{o}/\mathfrak{o}\}$$

can be expressed as

$$c = \prod_{\mathfrak{p} \mid g} j(\mathfrak{p}) \cdot h$$

where

$$j(\mathfrak{p}) = c(\mathfrak{o}_\mathfrak{p}/\mathfrak{o}_\mathfrak{p})$$

is the local class number and

$$h = h(k)$$

is the number of absolute classes of ideals in k. In particular

$$c < +\infty.$$

11. Irreducible representations. Let V be an irreducible representation space over k. The group $\mathfrak{G}$ is represented by automorphisms of V as

$$\mathfrak{G} \ni x \to A(x) \in GL(V; k).$$

Put the enveloping algebra

$$A_k = \sum_{x \in \mathfrak{G}} A(x)k \subseteq \mathfrak{E}(V; k)$$

and commuting algebra D defined by

$$D = \{S \mid \forall x \in \mathfrak{G};\ A(x)S = SA(x)\} \subseteq \mathfrak{E}(V; k)$$

where $\mathfrak{E}(V; k)$ is the endomorphism algebra of V over k. Since V is irreducible, D is a division algebra and A_k is a full matric algebra over the division algebra D^* inversely isomorphic to D.

PROPOSITION 11. 1. *Let M be a Γ-lattice in V, then*

$$\mathfrak{O} = \mathfrak{O}(M) = \{S \in D \mid MS \subseteq M\}$$

is an order in D.

PROOF. a) Since M is an $\mathfrak{o}$-module, $\mathfrak{O}$ contains $\mathfrak{o}$. b) Any element $S \in \mathfrak{O}$ is integral over $\mathfrak{o}$. For, let

$$f(S) = S^n + \alpha_1 S^{n-1} + \dots\dots + \alpha_n = 0 \ (\alpha_i \in k)$$

be the irreducible equation in k satisfied by S and $S = S^{(1)}, \dots\dots S^{(n)}$ be the conjugates of S over k. In the extended vector space

$$Vk(S^{(1)}, \dots\dots, S^{(n)})$$

we have

$$MS^{(i)} \subseteq M \qquad i = 1, \dots\dots, n.$$

Since α_i are symmetric functions of $S^{(j)}$'s we have

$$M\alpha_i \subseteq M.$$

Therefore $\alpha_i \in \mathfrak{o}$ by Prop. 10. 1.
c) $\mathfrak{O}k = D$. For, take an $S \in D$, $S \neq 0$, arbitrarily. Since

$$MS$$

is a Γ-lattice in V, we can find $\alpha \in \mathfrak{o}$ such that

$$MS\alpha \subseteq M.$$

This shows that $S\alpha \in \mathfrak{O}$. q. e. d.

We say that M is maximal if

$$\mathfrak{O} = \mathfrak{O}(M)$$

is a maximal order in D.

Any Γ-lattice can be embeded in a maximal Γ-lattice. Namely,

PROPOSITION 11. 2. *If $\mathfrak{O}^-$ is a maximal order containing $\mathfrak{O} = \mathfrak{O}(M)$, then*

$$M^- = M\mathfrak{O}^-$$

is a maximal Γ-lattice in V, with

$$\mathfrak{O}(M^-) = \mathfrak{O}^-.$$

PROOF. Since $\mathfrak{O}^-$ is a finite $\mathfrak{o}$-module, M^- is a lattice in V. From

$$MA(x) = M\mathfrak{O}^-A(x) = MA(x)\mathfrak{O}^- \subset M\mathfrak{O}^- = M^-$$

M^- is a Γ-lattice. And finally

$$M^-\mathfrak{O}^- = M\mathfrak{O}^-\mathfrak{O}^- = M\mathfrak{O}^- = M^-$$

implies

$$\mathfrak{O}(M^-) \supset \mathfrak{O}^-.$$

By Prop. 11.1 $\mathfrak{O}(M^{-1})$ is an order in D it follows from maximality of $\mathfrak{O}^-$ that

$$\mathfrak{O}(M^-) = \mathfrak{O}^-. \qquad \text{q. e. d.}$$

THEOREM 7. *If M is a maximal Γ-lattice in an irreducible representation space V over k, then the double cosets*

$$\widetilde{U}\,\widetilde{G}/G$$

of Theorem 5 *correspond in one to one way to the $\mathfrak{O} = \mathfrak{O}(M)$ left ideal classes in the commuting algebra D of $A(x)$'s.*

PROOF. Since $\mathfrak{O} = \mathfrak{O}(M)$ is a maximal order in D, G is the idèle group[11] of the division algebra D. The correspondences:

$$\widetilde{G} \ni \widetilde{S} \to \mathfrak{a}(\widetilde{S}) = \bigcap_{\mathfrak{p}} (\mathfrak{o}_{\mathfrak{p}} S_{\mathfrak{p}} \cap D) \subset D$$

are onto $\mathfrak{O}$-left ideals in D. Its kernel is just

$$\widetilde{U} = \{\widetilde{T} \mid M\widetilde{T} = M\} \text{ i. e. } \mathfrak{a}(\widetilde{T}\widetilde{S}) = \mathfrak{a}(\widetilde{S}).$$

Therefore, double cosets

$$\widetilde{U}\backslash\widetilde{G}/G$$

corresponds in one to one way to $\mathfrak{O}$-left ideal class i. e.

$$\mathfrak{a}(\widetilde{T}\widetilde{S}\cdot S) = \mathfrak{a}(\widetilde{S})\cdot S$$

with $\widetilde{T} \in \widetilde{U}$, $\widetilde{S} \in \widetilde{G}$, $S \in G$. q. e. d.

COROLLARY. *In addition to the assumptions on the Theorem* 7, *suppose D has degree* > 2 *or ramified infinite primes, then the class number*

$$\{M; k/\mathfrak{o}\} = \{M_1; \mathfrak{o}/\mathfrak{o}\} + \dots\dots + \{M_c; \mathfrak{o}/\mathfrak{o}\}$$

can be expressed as

$$c = \prod_{\mathfrak{p}|\mathfrak{g}} j(\mathfrak{p}) \cdot h$$

11) Cf. Fujisaki [11] for idèle group of a simple algebra.

where $j(\mathfrak{p}) = c(\mathfrak{o}_\mathfrak{p}/\mathfrak{o}_\mathfrak{p})$ *are local class numbes and* h *is the number of absolute ideal classes of the center* K *of* D.

PROOF. This follows from Theorem 7 and a theorem of Eichler[12] concerning class number of algebras. q. e. d.

THEOREM 8. *Let* M *be an arbitrary* Γ*-lattice in irreducible* V, *then the number of double cosets*

$$\widetilde{U}\backslash\widetilde{G}/G$$

is always finite.

PROOF. Let $M^- \supset M$ be a maximal Γ-lattice in V.
Then the number

$$\# \widetilde{U}^-\backslash\widetilde{G}/G,$$

as a class number of $\mathfrak{O}^- = \mathfrak{O}(M^-)$-left ideals of D, is finite.
Since $\widetilde{U}^- \supseteq \widetilde{U}$ it is sufficient to prove

$$[\widetilde{U}^- : \widetilde{U}] < +\infty.$$

Since $M^- \supseteq M$ are lattices, except for a finite set of primes we have

$$M_\mathfrak{p}^- = M_\mathfrak{p}$$

and hence

$$[U_\mathfrak{p}^- : U_\mathfrak{p}] = 1.$$

Take an exceptional prime $\mathfrak{p}$. $U_\mathfrak{p}^- \supseteq U_\mathfrak{p}$ are compact and open subgroups in $D_\mathfrak{p}^{[1)}$, therefore

$$[U_\mathfrak{p}^- : U_\mathfrak{p}] < +\infty. \qquad \text{q. e. d.}$$

12. Some examples. Let $\mathfrak{G} = \mathbf{Z}/(n)$ be a cyclic group of order n. Consider faithful irreducible integral representation in the field of rationals $\mathbf{Q}$.

Let V be a representation space of dimension

$$m = \varphi(n)$$

$$A_k = \sum_{i=0}^{n-1} A(x^i)\mathbf{Q} = D \simeq K = \mathbf{Q}(\zeta)$$

where ζ is a primitive n-th roots of unity.

It is readily seen that

$$A_k \ni A(x) \to \zeta \in K$$

is an isomorphism over $\mathbf{Q}$, if $x \in \mathfrak{G}$ is a fixed generator.

PROPOSITION 12. 1. *Any* Γ*-lattice* M *in* V *is maximal.*

12) Eichler [9], $n=2$ and total definite case was also treated by him [8].

PROOF. By definition

$$\mathfrak{O} = \{S \in D \mid MS \subset M\}.$$

As a Γ-module:

$$MA(x^i) \subseteq M$$

therefore we have

$$\mathfrak{O} \supseteq \sum_{i=0}^{n-1} A(x^i)\mathbf{Z}.$$

Since $\mathbf{Z}[\zeta] = \sum_{i=0}^{n-1} \zeta^i\mathbf{Z}$ is the maximal order of $K = \mathbf{Q}(\zeta)$ we see that

$$\mathfrak{O} = \sum_{i=0}^{n-1} A(x^i)\mathbf{Z}$$

is the maximal order of D. q. e. d.

The class number defined by

$$\{M; \mathbf{Q}/\mathbf{Z}\} = \{M_1; \mathbf{Z}/\mathbf{Z}\} + \dots\dots + \{M_c; \mathbf{Z}/\mathbf{Z}\}$$

is therefore given by

$$c = \prod_{p \mid n} j(p) \cdot h$$

where

$$h = h(\mathbf{Q}(\zeta))$$

is the absolute ideal class number of the field of n-th roots of unity. Now consider $j(p)$. If n is a prime power and

$$n \equiv 0 \ (p)$$

then

$$(p-1, n) = 1$$

i. e. $GF(p)$ contains no n-th roots. Therefore p-modular representation of $A(x)$ for $n \equiv 0 \ (p)$ are irreducible. By a theorem of Brauer[13)]

$$j(p) = 1$$

And hence

$$c = h.$$

As a next example, consider the symmetric group

$$\mathfrak{S}_3$$

of order $g = 6$ in the field of rationals $\mathbf{Q}$. Let $A(x)$ be the 2-dimensional absolutely irreducible representation with Γ-lattice M.

13) Brauer [4], Theorem 10 or Artin-Nesbitt-Thrall [1], Lemma 9. 8 D.

If $p = 2$,

$$\frac{6}{2} = 3 \not\equiv 0 \ (2)$$

implies that $A(x)$ is irreducible mod 2, therefore[13]

$$j(2) = 1.$$

If $p = 3$, $A(x)$ is reducible mod 3 and contains two modular irreducible constituents. Therefore by a deep theorem of Brauer[14]

$$j(3) = 2.$$

Finally, since $h(\mathbf{Q}) = 1$, we have

$$c = \prod_{p|6} j(p) = j(3) = 2.$$

BIBLIOGRAPHY

[1] E. ARTIN-C. J. NESBITT-R. M. THRALL, Rings with minimum condition. Ann Arbor 1944

[2] L. BIEBERBACH, Ueber die Minkowskische Reduktion der positiven quadratischen Formen und die endlichen Gruppen linearer ganzzahliger Substitutionen. Gött. Nach. 1912, 207–216.

[3] R. BRAUER, On modular and $\mathfrak{p}$-adic representations of algebras. Proc. N. A. S. 25(1939), 252–258.

[4] R. BRAUER, Investigations on group characters. Ann. of Math. 42(1941), 936–958.

[5] R. BRAUER, Zur Darstellungstheorie der Gruppen endlicher Ordnung. Math. Zeitschr. 63(1956), 406–444.

[6] C. CHEVALLEY, L'arithmétique dans les algèbres des matrices. Actualités Sci. et Ind. 323(1936).

[7] F. E. DIEDERRICHSEN, Ueber die Ausreduktion ganzzahliger Gruppendarstellungen bei arithmeticher Aequivalenz. Hamb. Abh. 13(1939), 357–412.

[8] M. EICHLER, Ueber die Idealklassenzahl total definiter Quaternionenalgebren. Math. Zeitschr. 43(1938), 102–109.

[9] M. EICHLER, Ueber die Idealklassenzahl hyperkomplexer Systeme. Math. Zeitschr. 43 (1938), 481–494.

[10] M. EICHLER, Quadratische Formen und orthogonale Gruppen. Berlin 1952.

[11] G. FUJISAKI, On the zeta-function of the simple algebra over the field of rational numbers. J. Faculty of Sci. Univ. of Tokyo, Sec. I, VII(1958) 567–604.

[12] W. GASCHUETZ, Ueber den Fundamentalsatz von Maschke zur Darstellungstheorie der endlichen Gruppen. Math. Zeitschr. 56(1952), 379–387.

[13] C. JORDAN, Mémoire sur l'équivalence des formes. Journ. éc. pol. XXIX, 1880.

[14] H. KUNIYOSHI-S. TAKAHASHI, On the principal genus theorem. Tohoku Math. J. 5(1953) 128–131.

[15] J. M. MARANDA, On $\mathfrak{p}$-adic integral representations of finite groups. Canad. J. of Math. 5(1953) 344–355.

[16] J. M. MARANDA, On the equivalence of representations of finite groups by groups of automorphisms of modules over Dedekind rings. Canad. J. of Math. 7(1955), 516–526.

[17] T. ONO, Sur une propriété arithmétique des groupes algébriques commutatifs. Bull. Soc. Math. France 85(1957), 307–323,

14) Brauer [4], Theorem 11,

[18] I. REINER, Maschke modules over Dedekind rings. Canad. J. of Math. 8(1956), 329–334.
[19] I. REINER, Integral representations of cyclic groups of prime order. Proc. A. M. S. 8 (1957) 142–146.
[20] A. SPEISER, Die Theorie der Gruppen von endlicher Ordnung. Berlin, 3 Aufl. 1937.
[21] H. ZASSENHAUS, Neuer Bewsis der Endlichkeit der Klassenzahl bei unimodularer Aequivalenz endlicher ganzzahliger Substitutionsgruppen. Hamb. Abh. 12(1937–1938), 276, –288.

MATHEMATICAL INSTITUTE, TÔHOKU UNIVERSITY.