PHILOSOPHICAL TRANSACTIONS OF THE ROYAL SOCIETY A MATHEMATICAL, PHYSICAL & ENGINEERING SCIENCES

The Rational Characterization of Certain Sets of Relatively Abelian Extensions

A. Frohlich

Phil. Trans. R. Soc. Lond. A 1959 **251**, 385-425
doi: 10.1098/rsta.1959.0007

THE RATIONAL CHARACTERIZATION OF CERTAIN SETS OF RELATIVELY ABELIAN EXTENSIONS

By A. FRÖHLICH
King's College, University of London

(*Communicated by H. A. Heilbronn, F.R.S.—Received* 3 *December* 1957)

CONTENTS

Let H be a class group—in the sense of class-field theory— in the rational field P, whose order is some power of a prime l. With H there is associated an Abelian extension K of P. The purpose of this paper is to determine in rational terms and for all fields K given in the described manner, the set $\mathfrak{C}(K/P)$ of cyclic extensions Λ of K of relative degree l, which are absolutely normal.[†] In particular we shall find the ramification laws for these fields Λ, and the possible extension types of a group of order l by the Galois group of K, which are realized in Galois groups of fields in $\mathfrak{C}(K/P)$. It is fundamental to the programme outlined, that we aim at obtaining purely rational criteria of determination.

Introduction

As an introduction to the subject matter of this paper, some of the questions we are interested in and some of the results, will be illustrated in terms of a particular case. We shall avoid at this stage, as far as possible, bringing in the formal concepts which will eventually be used, and instead give a simple, *ad hoc* description of the example considered.

Let K be an absolutely Abelian, non-cyclic field of degree 4, and let $\mathfrak{C}(K)$ be the set of absolutely normal fields Λ of at most degree 8 which contain K. Such a field Λ either coincides with K or is relative quadratic over K. In the latter case the absolute Galois group of Λ is defined in a natural manner as an extension of a group E of order 2 by the Galois group Γ of K. There thus corresponds to each field Λ in $\mathfrak{C}(K)$ a factor-system class of Γ in E; this correspondence can be extended so as to cover also the case $\Lambda = K$, associating with this field the unit class. The question then arises: which of the factor-system classes of Γ in E are realized in the manner described by fields in $\mathfrak{C}(K)$? One can show that these

[†] Later K also will be formally included in $\mathfrak{C}(K/P)$.

classes form a group $A(\mathrm{K})$. Our first aim is to determine $A(\mathrm{K})$ in *purely rational* terms. To formulate the answer concretely E is taken as the group of square roots of unity and an explicit representation of the factor-system classes of Γ in E will be introduced.

K is the union of two quadratic fields whose discriminants are D_1 and D_2. Γ is then generated by elements γ_1, γ_2 such that for $i, j = 1, 2$

$$\gamma_i \sqrt{D_j} = (-1)^{\delta_{ij}} \sqrt{D_j}.$$

In the extension $\bar{\Gamma}$ of E by Γ choose representatives $\bar{\gamma}_i$ of γ_i. We obtain relations

$$\bar{\gamma}_i^2 = (-1)^{C(\gamma_i)} \quad (i = 1, 2); \qquad \bar{\gamma}_1^{-1}\bar{\gamma}_2^{-1}\bar{\gamma}_1\bar{\gamma}_2 = (-1)^{C(\gamma_1, \gamma_2)}.$$

The exponents taken mod 2 do not depend on the choice of representatives and determine the structure of $\bar{\Gamma}$. Moreover, each triplet $\bar{c} = [C(\gamma_1), C(\gamma_2), C(\gamma_1, \gamma_2)]$ defines some extension of E by Γ. The set of all such triplets $\bar{c}$ with component-wise addition mod 2 is thus precisely the group of factor-system classes of Γ in E, and we have

$\bar{c}$ is realized by some field Λ in $\mathfrak{C}(\mathrm{K})$ (i.e. $\bar{c}$ belongs to the subgroup $A(\mathrm{K})$), if and only if

$$\text{(A)} \qquad \left(\frac{D_1, D_2}{p}\right)^{C(\gamma_1, \gamma_2)} \left(\frac{-1, D_1}{p}\right)^{C(\gamma_1)} \left(\frac{-1, D_2}{p}\right)^{C(\gamma_2)} = 1, \quad \textit{for all } p.$$

We see that this criterion is a 'finite' one, as (A) is trivially satisfied if p is non-ramified in K.

Assume now that the factor-system class $\bar{c}$ satisfies (A). We then ask: what can be said about the ramification of rational primes in the fields Λ belonging to $\bar{c}$? Not unexpectedly the discriminant prime divisors of K play a special role. Their ramification in the relative extension Λ/K is in a very strong sense determined by $\bar{c}$; an explicit criterion involving only the components of $\bar{c}$ and the rational quadratic residue characters associated with K can be derived. On the other hand, one can—within the obvious limitation—prescribe arbitrarily the ramification behaviour of all other primes. In particular, we have

Every factor-system class $\bar{c}$ satisfying (A) is realized by a field Λ whose discriminant prime divisors are precisely those of K.

Among these fields those for which $\bar{c}$ is the unit class are of particular importance. These are the fields $\mathrm{K}(\sqrt{D})$, where $D = 1$, or D is a quadratic discriminant in the rational field all of whose prime divisors are ramified in K.

A more detailed characterization of this ramification law can be given in terms of rational quadratic residue characters whose conductor is prime to the discriminant of K. To each field there corresponds in a natural manner such a character χ, and the conductor prime divisors of χ are precisely those primes ramified in Λ but not in K. Moreover, if χ is a character of this type—possibly the trivial character—and if $\bar{c}$ lies in $A(\mathrm{K})$ then there exists a field in $\mathfrak{C}(\mathrm{K})$ belonging—in the obvious sense described—to the pair $(\chi, \bar{c})$; the number of such fields is the same as the number of fields $\mathrm{K}(\sqrt{D})$ mentioned above.

Having associated with each field Λ a pair $(\chi, \bar{c})$, we are now led to the problem of characterizing the fields in $\mathfrak{C}(\mathrm{K})$ by rational invariants. At this stage it becomes worth while to introduce the formal description of the set $\mathfrak{C}(\mathrm{K})$ by the character group $\Phi(\bar{\Lambda}/\mathrm{K})$ which will be used throughout this paper. Here $\bar{\Lambda}$ is the union of the fields in $\mathfrak{C}(\mathrm{K})$. The elements of this group can be interpreted either as idèle class characters in K or as continuous characters of the Galois group of $\overline{\Lambda}/\mathrm{K}$. Our problem is then to determine this group rationally in a way which exhibits the field-theoretic and arithmetic properties of its elements and of the corresponding fields.

One can now associate with each character ϕ in $\Phi(\overline{\Lambda}/\mathrm{K})$ a pair $(\chi_\phi, \bar{c}_\phi)$ of the type considered already, and each such pair $(\chi, \bar{c})$ is associated with some ϕ. The mappings $\phi \rightarrow \bar{c}_\phi$, $\phi \rightarrow \chi_\phi$ are homomorphisms. Finally, the group of characters ϕ for which χ_ϕ, $\bar{c}_\phi$ are the unit elements, is finite and can be easily determined. Thus when D_1, D_2 are odd this is the classical group of genus characters of K.

The type of problem with which we are concerned has been indicated in the preceding discussion. The class of fields covered in this paper is given by the following data: The base field is as before the rational field P; l is a natural prime and K is an Abelian extension of P, given by its class group in P, whose degree is some power of l; $\mathfrak{C}(\mathrm{K}/\mathrm{P}) = \mathfrak{C}(\mathrm{K})$ is the set of all fields Λ which are normal over P and of relative degree l (or 1) over K. The same methods could also be used under less restrictive conditions, allowing K to be any Abelian field and $\mathfrak{C}(\mathrm{K}/\mathrm{P})$ the set of central extensions of K. On the other hand, we could take the base field P as a rational p-adic field, and we shall in fact briefly touch upon this case. The first half of this paper applies to any base field P which is a finite algebraic number field; the author hopes to return to a complete treatment of this more general problem.

The first stage in our programme is to obtain a suitable description of $\mathfrak{C}(\mathrm{K}/\mathrm{P})$ by what one may call formal description invariants. These are (i) groups of characters which will in the first place be interpreted as characters of Galois groups—see, for example, the group $\Phi(\overline{\Lambda}/\mathrm{K})$ already mentioned, (ii) a group $A(\mathrm{K})$ of factor-system classes representing group extensions which are realized by fields in $\mathfrak{C}(\mathrm{K}/\mathrm{P})$. These groups are then connected by an exact sequence S of homomorphisms. So far no restriction has to be imposed on the base field. If, however, P admits a class-field theory the terms and mappings of S acquire an immediate arithmetic meaning. Moreover, if P is a finite algebraic number field, then for each prime divisor $\mathfrak{p}$ in P one can derive an exact sequence $S_\mathfrak{p}$, which is a homomorphic image of S.

The contents of §§ 4, 5 do not form an integral part of our investigation, but supplement it. § 4 contains a detailed interpretation of the formal description invariants in terms of class-field theory over K, and in § 5 these invariants are briefly discussed from the point of view of Kummer theory. The final results can thus be interpreted as providing a rational determination of structural properties of the idèle class group, and if $l = 2$, of the multiplicative group, in K.

In the second half of the paper (§§ 7 to 13) the base field is the rational field. A rational characterization of the groups involved in the formal description of $\mathfrak{C}(\mathrm{K}/\mathrm{P})$ will be derived. One wants, of course, to determine these groups not just in the abstract sense, but as concretely given groups of elements with certain definite arithmetic properties. This approach was typified in the example discussed earlier on. The central role is played here by (i) the residue characters associated with the characters of $\Phi(\overline{\Lambda}/\mathrm{K})$ and the ramification laws described by these, (ii) the group $A(\mathrm{K})$ of factor-system classes realized in $\mathfrak{C}(\mathrm{K}/\mathrm{P})$. In the particular case we have considered, the conditions (A) for $A(\mathrm{K})$ were formulated in terms of a basis of Γ; analogous explicit conditions will be derived in the general case, using however, residue characters instead of the norm residue symbol which will not always be at our disposal. Moreover, an invariant criterion for $A(\mathrm{K})$ will be obtained, which does not depend on any choice of basis. As an illustration the abstract groups which appear as Galois groups of fields in $\mathfrak{C}(\mathrm{K}/\mathrm{P})$ will be determined in some simple cases in the final section.

The problem of decomposition of rational primes in the fields considered will only briefly be touched upon. An explicit decomposition law for all fields of the type considered here is not known. It will, however, be shown in a subsequent publication, based on the present paper, that such a law can be formulated for the fields in $\mathfrak{C}(\mathrm{K}/\mathrm{P})$, if, for example, K is of the type considered in our example.

In conclusion, there follow a few remarks on the general background of this paper. The problem we are concerned with is of the following type: we are given a field P, to be more definite say a finite algebraic number field, and a finite normal algebraic extension K of P; a set $\mathfrak{C}(\mathrm{K}/\mathrm{P})$ of fields Λ which are normal algebraic over P and Abelian over K is defined by prescribing some property of these fields, such as their degree. We then wish to determine in some sense the set $\mathfrak{C}(\mathrm{K}/\mathrm{P})$ and to characterize the relative behaviour of its fields with respect to K and to P. Once one attempts to formulate this aim more precisely one is immediately led to a fundamental distinction between two possible types of characterization, namely, either in terms of K or in terms of P. In the first approach K is taken as known in the sense that any of its structural properties may be presupposed. Results of a general nature have been obtained in this direction (Brauer 1947; Hasse 1947, 1948; Jehne 1952; Wolf 1953*a*, *b*, 1956). Thus, in his fundamental paper Hasse (1947) treats the problem both from the point of view of class-field theory and from the point of view of Kummer theory and derives under the appropriate hypothesis a complete set of Kummer invariants in K. Since then new developments in class-field theory (Weil 1951; Nakayama 1952; Hochschild & Nakayama 1952; Jehne 1952) have brought problems of characterization in K within the scope of this theory. The essential step was the discovery of the canonical factor-system class of K over P; in fact the Artin mapping over K maps this class onto the operative factor-system class of $\Lambda/\mathrm{K}/\mathrm{P}$ in the sense of § 2.

Here we are, however, concerned with the essentially different question of a characterization in the base field P. K is now given only in a very restricted sense, namely by its associated class group H_{K} in P. Beyond that the structure of K is not assumed to be known and does not enter the criteria of determination which are to be formulated solely in terms of P. What we thus really consider is a whole family of class groups H_{K}, with each a set $\mathfrak{C}(\mathrm{K}/\mathrm{P})$ being associated. As far as algebraic number fields are concerned very little is known on problems of this type, except of course in the case when $\mathfrak{C}(\mathrm{K}/\mathrm{P})$ consists by definition only of class fields of P. It seems thus worth while to try to obtain a solution for some restricted class of algebraic number fields; this will be done here. Some results in this direction have been found incidentally by Scholz (1929, 1936), Reichardt (1936, 1937) and Šafarevič (1954*a*, *b*, *c*) in the course of their investigations on the existence of fields with a given soluble Galois group.†

† (*Note added* 29 *January* 1959). The author has now succeeded in obtaining a generalization of the theory, as developed in the second half of this paper; this covers situations in which a finite algebraic number field—in place of the rational field—is taken as the base field. This is done by a new approach via the corresponding local theory. A detailed account of the rational case seems however still to be desirable, in particular as a good many of the results depend specifically on the rational field as base field and extend either only in a weakened form, or not at all to more general base fields.

1. The character group of an Abelian extension field

We denote the Galois group of a normal algebraic extension field $\overline{\mathrm{M}}$ of a field M by $\Gamma(\overline{\mathrm{M}}/\mathrm{M})$. Assume that $\overline{\mathrm{M}}$ is an Abelian extension of M. We denote the group of continuous characters of the Galois group $\Gamma(\overline{\mathrm{M}}/\mathrm{M})$ by $\Phi(\overline{\mathrm{M}}/\mathrm{M})$, and if $\overline{\mathrm{M}}$ is the maximal Abelian extension of M also by $\Phi(\mathrm{M})$. If M_1 is a field between M and $\overline{\mathrm{M}}$ we shall consider $\Phi(\mathrm{M}_1/\mathrm{M})$ as a subgroup of $\Phi(\overline{\mathrm{M}}/\mathrm{M})$. The mapping $\mathrm{M}_1 \rightarrow \Phi(\mathrm{M}_1/\mathrm{M})$ is a biunique mapping of the set of fields between M and $\overline{\mathrm{M}}$ onto the set of subgroups of $\Phi(\overline{\mathrm{M}}/\mathrm{M})$ with the following properties:

(i) It induces a lattice isomorphism of the lattice of fields between M and $\overline{\mathrm{M}}$ onto the lattice of subgroups of $\Phi(\overline{\mathrm{M}}/\mathrm{M})$, both lattices having inclusion as their defining order relation.

(ii) An element γ of $\Gamma(\overline{\mathrm{M}}/\mathrm{M})$ leaves the field M_1 element-wise fixed if and only if $\phi(\gamma) = 1$ for all $\phi \in \Phi(\mathrm{M}_1/\mathrm{M})$.

(iii) A character ϕ in $\Phi(\overline{\mathrm{M}}/\mathrm{M})$ satisfies $\phi(\gamma) = 1$ for all γ leaving M_1 element-wise fixed, if and only if $\phi \in \Phi(\mathrm{M}_1/\mathrm{M})$.

(iv) If $\Phi(\mathrm{M}_1/\mathrm{M})$ or $\Gamma(\mathrm{M}_1/\mathrm{M})$ is finite, then $\Phi(\mathrm{M}_1/\mathrm{M}) \cong \Gamma(\mathrm{M}_1/\mathrm{M})$.

We shall, when $\Phi = \Phi(\mathrm{M}_1/\mathrm{M})$ also write $\mathrm{M}_1 = \mathrm{M}_\Phi$, and for cyclic Φ, $\mathrm{M}_1 = \mathrm{M}_\phi$ if ϕ is a generator of Φ.

Let now Λ be normal over a field M, and let $\overline{\Lambda}$ and $\overline{\mathrm{M}}$ be the maximal Abelian extensions of Λ and of M, respectively. Then $\overline{\mathrm{M}} \subseteq \overline{\Lambda}$ and $\Gamma(\overline{\mathrm{M}}/\mathrm{M}) = \Gamma(\overline{\Lambda}/\mathrm{M})/\Gamma(\overline{\Lambda}/\overline{\mathrm{M}})$. If $\phi \in \Phi(\mathrm{M})$, $\gamma \in \Gamma(\overline{\Lambda}/\Lambda)$ we write $\phi'(\gamma) = \phi(\gamma\Gamma(\overline{\Lambda}/\overline{\mathrm{M}}))$. Then $\phi' \in \Phi(\Lambda)$, and the mapping $R_{\mathrm{M}/\Lambda}$: $\phi \rightarrow \phi'$ is a homomorphism of $\Phi(\mathrm{M})$ into $\Phi(\Lambda)$.

If M is a finite algebraic extension of the rational field or of some local completion of that field, then class-field theory asserts the existence of a canonical isomorphism of $\Phi(\mathrm{M})$ onto the group of class-group characters of M (Chevalley 1940). We shall in fact identify the two groups of characters. For algebraic number fields we shall use the idèle-theoretic formulation of class-field theory here (see, for example, Chevalley 1940, 1954). The convention to be made is then: if M is a finite algebraic extension of the rational field (of a local completion of the rational field), and if $\phi \in \Phi(\mathrm{M})$, then we interpret ϕ as a function of idèles (of non-zero elements of M) by the rule

$$\phi(\mathfrak{A}) = \phi((\mathrm{M}_\phi/\mathrm{M}; \mathfrak{A})),$$

where $(\Lambda/\mathrm{M}; \mathfrak{A})$ is the Artin symbol. Thus when M is an algebraic number field, ϕ is considered as a character of the idèle group, which is effectively an idèle class character (or differential).

2. Factor systems and central extension fields

Let Γ be a group and let Δ be an Abelian group such that Γ is realized in a given manner as a group of automorphisms of Δ. Throughout, this realization of Γ by automorphisms of Δ will be the trivial one, i.e. each element of Γ is assumed to induce the identical automorphism on Δ. We denote the group of factor systems of Γ in Δ by $F(\Gamma, \Delta)$; $F(\Gamma, \Delta)$ is thus the group of mappings a: $\Gamma \times \Gamma \rightarrow \Delta$ satisfying

$$a(\gamma_1, \gamma_2)\, a(\gamma_1\gamma_2, \gamma_3) = a(\gamma_1, \gamma_2\gamma_3)\, a(\gamma_2, \gamma_3), \tag{2·1}$$

for all $\gamma_1, \gamma_2, \gamma_3 \in \Gamma$. The elements a in $F(\Gamma, \Delta)$ for which there exists a mapping $b: \Gamma \to \Delta$ with

$$a(\gamma_1, \gamma_2) = b(\gamma_1)\, b(\gamma_2)\, (b(\gamma_1 \gamma_2))^{-1} \tag{2·2}$$

form a subgroup of $F(\Gamma, \Delta)$. The coset or class of a factor system a modulo this subgroup will be denoted by $\bar{a}$, and the group of factor-system classes by $\bar{F}(\Gamma, \Delta)$.

Let† Ω be a group, and let‡

$$[\Omega, t, s]: \quad 1 \to \Delta \xrightarrow{t} \Omega \xrightarrow{s} \Gamma \to 1$$

be an exact sequence of homomorphisms. If r is a biunique mapping of Γ into Ω such that $s(r(\gamma)) = \gamma$, for all $\gamma \in \Gamma$, then $r(\Gamma)$ is a complete set of representatives of Γ in Ω, and for all $\gamma_1, \gamma_2 \in \Gamma$ there exists an element $a(\gamma_1, \gamma_2) \in \Delta$, such that

$$r(\gamma_1)\, r(\gamma_2) = t(a(\gamma_1, \gamma_2))\, r(\gamma_1 \gamma_2). \tag{2·3}$$

a is an element of $F(\Gamma, \Delta)$. Thus to every quadruplet $[\Omega, t, s, r]$ of the form described there corresponds by (3) an element a of $F(\Gamma, \Delta)$. For given $[\Omega, t, s]$ and varying r, the element a will vary over a given class in $\bar{F}(\Gamma, \Delta)$. There thus corresponds to each sequence $[\Omega, t, s]$ a unique element $\bar{a}$ of $\bar{F}(\Gamma, \Delta)$, which will be called the operative factor-system class of $[\Omega, t, s]$. Two sequences $[\Omega, t, s]$ and $[\Omega', t', s']$ have the same operative factor-system class if and only if there exists an isomorphism v of Ω onto Ω', such that

$$vt = t', \quad s = s'v. \tag{2·4}$$

Two sequences connected in this manner are said to be of the same type in the strong sense. Assume in particular that M and K are normal extensions of a field P, and that M is an Abelian extension of K, such that $\Gamma(\mathrm{M/K}) = \Delta$ lies in the centre§ of $\Gamma(\mathrm{M/P}) = \Omega$. Then the realization of $\Gamma(\mathrm{K/P}) = \Gamma$ as a group of automorphisms of Δ which is induced by the group Ω in the obvious manner is the trivial one. Furthermore, the mappings t and s are given in a natural manner. t is the injection mapping of $\Gamma(\mathrm{M/K})$ into $\Gamma(\mathrm{M/P})$, and s is given by restricting each automorphism of M over P to the field K. In this case one need not specify s and t explicitly, and one can simply speak of the operative factor-system class in $\bar{F}(\Gamma(\mathrm{K/P}), \Gamma(\mathrm{M/K}))$ for the group $\Gamma(\mathrm{M/P})$, or of the operative factor-system class for M/K/P.

Weakening the relation (2·4) two exact sequences $[\Omega, t, s]$ and $[\Omega', t', s']$ are said to be of the same type in the weak sense, if there exists an isomorphism v of Ω onto Ω', and an automorphism g of Δ such that

$$vt = t'g, \quad s = s'v. \tag{2·5}$$

This equivalence relation is still stronger than that of an isomorphy $\Omega \cong \Omega'$. Assume now that two elements a_1 and a_2 of $F(\Gamma, \Delta)$ are related by

$$a_2(\gamma_1, \gamma_2) = g(a_1(\gamma_1, \gamma_2)), \quad \text{for all} \quad \gamma_1, \gamma_2 \in \Gamma, \tag{2·6}$$

g being an automorphism of Δ. The mapping $\bar{g}: \bar{a}_1 \to \bar{a}_2$ of $\bar{F}(\Gamma, \Delta)$ into itself, given by (2·6) for fixed g is uniquely defined, and is an automorphism of $\bar{F}(\Gamma, \Delta)$. The set of all elements $\bar{g}\bar{a}$ for any given class $\bar{a}$ and for all automorphisms g of Δ, will be called the type of $\bar{a}$. The

† The following discussion applies essentially also—with appropriate changes—to the general case not considered here, when Γ operates on Δ not necessarily in a trivial manner.

‡ It will be recalled that a sequence of homomorphisms is exact, if for each 'step' $\xrightarrow{g} A \xrightarrow{f}$, the image group of g is the kernel of f. Thus $1 \to A \xrightarrow{f} B$ is exact, if and only if f is an isomorphism into B, and $B \xrightarrow{g} A \to 1$ is exact, if and only if g is a homomorphism *onto* A.

§ In such a situation M is said to be a central extension of K over P.

types are thus equivalence classes on $\overline{F}(\Gamma, \Delta)$; two elements $\bar{a}_1$, and $\bar{a}_2$ belong to the same type if and only if (2·6) holds for some representative a_i of $\bar{a}_i$ $(i = 1, 2)$ and for some g. The type of the operative factor-system class of $[\Omega, t, s]$ will be called the operative type of $[\Omega, t, s]$. It is easy to see now that the two exact sequences are of the same type in the weaker sense, if and only if their operative types coincide.

When K is a normal extension of a field P and M a central extension of K over P we can again simply speak of the operative type of M/K/P. This concept arises naturally when one considers sets of fields, with certain prescribed properties.† Assume for simplicity's sake that K is a normal extension of a field P, and that $\mathfrak{C}$ is the set of all central extensions M of K over P, such that Γ(M/K) is isomorphic to a given group Δ. For M ∈ $\mathfrak{C}$, the group Γ(M/K) is then merely given as an abstract group, but not explicitly as a group of field automorphisms. The choice of the particular homomorphism t is thus still open; more precisely, the defining conditions of $\mathfrak{C}$ prescribe merely the set $[tg]$, where t is a fixed homomorphism $\Delta \to \Omega$ and g varies over the automorphisms of Δ. The operative factor-system classes for M/K/P, as M varies over $\mathfrak{C}$, can thus from the nature of the problem only be determined to within their type. Once it is realized, however, that in problems of this nature the operative type is the fundamental concept the procedure used can be considerably simplified. We need not consider simultaneously all the groups $\overline{F}(\Gamma(\mathrm{K/P}), \Gamma(\mathrm{M/K}))$ as M varies over $\mathfrak{C}$, but can restrict ourselves to the one group $\overline{F}(\Gamma(\mathrm{K/P}), \Delta)$ and speak of the operative type for M/K/P in that group. In fact let $\Delta \cong \Delta'$ and let h be an isomorphism of Δ onto Δ′. Then if $a \in F(\Gamma, \Delta)$, the equations

$$[h^*a]\,(\gamma_1, \gamma_2) = h(a(\gamma_1, \gamma_2))$$

will determine an element $h^*a \in F(\Gamma, \Delta')$. Here $\overline{h^*a}$ depends solely on $\bar{a}$, and the mapping $\bar{h}$: $\bar{a} \to \overline{h^*a}$ is an isomorphism of $\overline{F}(\Gamma, \Delta)$ onto $\overline{F}(\Gamma, \Delta')$. The image of a type in $\overline{F}(\Gamma, \Delta)$ is a type in $\overline{F}(\Gamma, \Delta')$, and this image type does not depend on the particular choice of h.

Assume from now Γ to be a finite Abelian group. Denote the order of an element γ by n_γ. A mapping c: $\Gamma \times \Gamma \to \Delta$ will be called a commutator factor system of Γ in Δ, if

$$\left.\begin{aligned} &c(\gamma_1, \gamma_2) = (c(\gamma_2, \gamma_1))^{-1}, \quad c(\gamma, \gamma) = 1, \\ &c(\gamma\gamma_1, \gamma_2) = c(\gamma, \gamma_2)\, c(\gamma_1, \gamma_2), \quad c(\gamma, \gamma_1\gamma_2) = c(\gamma, \gamma_1)\, c(\gamma, \gamma_2), \end{aligned}\right\} \tag{2·7}$$

for all $\gamma, \gamma_1, \gamma_2 \in \Gamma$. A consequence of (2·7) is the equation $c(\gamma, \gamma_1)^{n_\gamma} = c(\gamma_1, \gamma)^{n_\gamma} = 1$. The commutator factor systems form a group $C(\Gamma, \Delta)$. If a is an element of $F(\Gamma, \Delta)$, then the function a_* defined by $a_*(\gamma_1, \gamma_2) = a(\gamma_1, \gamma_2)\,(a(\gamma_2, \gamma_1))^{-1}$ is an element of $C(\Gamma, \Delta)$. We shall construct below an element a of $F(\Gamma, \Delta)$ such that a_* is a prescribed element of $C(\Gamma, \Delta)$. It follows that the mapping $a \to a_*$ is a homomorphism of $F(\Gamma, \Delta)$ onto $C(\Gamma, \Delta)$.

Next define corresponding to each element a in $F(\Gamma, \Delta)$ a mapping a^*: $\Gamma \to \Delta$, called the power-factor system corresponding to a, by the rule $a^*(\gamma) = \prod_{r \bmod n_\gamma} a(\gamma, \gamma^r)$ for all $\gamma \in \Gamma$.‡ The power-factor systems form a group $P(\Gamma, \Delta)$, which is a homomorphic image of $F(\Gamma, \Delta)$ under the mapping $a \to a^*$. From (2·2) we deduce by direct calculation that for $a \in F(\Gamma, \Delta)$, $\bar{a} = 1$ if and only if $a_* = 1$, and $a^*(\gamma) \equiv 1 \pmod{\Delta^{n_\gamma}}$ for all $\gamma \in \Gamma$. It will be assumed throughout that $a(1, 1) = 1$ whence $a^*(1) = 1$.

† This was pointed out by Hasse (1947).

‡ The power-factor systems can be characterized directly by equations involving also commutator factors, but this characterization will not be used, and therefore will be omitted.

Let now $\mathfrak{g} = [\gamma_1, \ldots, \gamma_m]$ be a basis of Γ; denote the order of γ_i by n_i and write $(n_i, n_j) = n_{ij}$. Then one verifies easily that $a^*(\gamma) \bmod \Delta^{n_\gamma}$, for all $\gamma \in \Gamma$, and a^* are uniquely determined by the elements $a^*(\gamma_i)$ $(i = 1, \ldots, m)$, and $a_*(\gamma_i, \gamma_j)$ for $i<j$.† Conversely let $c(\gamma_i, \gamma_j)$ for $1 \leqslant i < j \leqslant m$ be elements of Δ satisfying $c(\gamma_i, \gamma_j)^{n_{ij}} = 1$, and let $b(\gamma_i)$ $(i = 1, \ldots, m)$ be arbitrary elements of Δ. Define for $i = 1, \ldots, m$ a function $o_i(s, r)$ on pairs of integers (s, r) as follows: put $s_i \equiv s$, $r_i \equiv r \pmod{n_i}$, $0 \leqq s_i$, $r_i < n_i$ and put $o_i(s, r) = 0$, or $= 1$, according to whether $s_i + r_i < n_i$, or $s_i + r_i \geqq n_i$. Write for all systems of exponents q_i, t_i $(i = 1, \ldots, m)$‡

$$a\left(\prod_{i=1}^{m} \gamma_i^{t_i}, \prod_{i=1}^{m} \gamma_i^{q_i}\right) = \prod_{i=1}^{m} b(\gamma_i)^{o_i(t_i, q_i)} \prod_{i<j} c(\gamma_i, \gamma_j)^{q_i t_j}. \tag{2·8}$$

Then a is a uniquely defined mapping $\Gamma \times \Gamma \rightarrow \Delta$ and it is easily verified that $a \in F(\Gamma, \Delta)$. We see that $a_* = c^{-1}$, where c is the unique element of $C(\Gamma, \Delta)$ with the prescribed values $c(\gamma_i, \gamma_j)$ $(i<j)$, and that $a^*(\gamma_i) \equiv b(\gamma_i) \bmod \Delta^{n_i}$ $(i = 1, \ldots, m)$. The construction described thus enables us to obtain factor systems out of any given class $\bar{a}$. Moreover, if for $i = 1, \ldots, m$, the group Δ^{n_i} only contains the unit element, the elements $c(\gamma_i, \gamma_j)$ can be arbitrarily prescribed, and distinct systems of prescribed invariants $c(\gamma_i, \gamma_j)$, $b(\gamma_i)$ will lead to factor systems in distinct classes.

If a is given by (2·8) then in particular

$$a(\gamma_i, \gamma_i^{-1}) = b(\gamma_i), \quad a(\gamma_j, \gamma_i) = c(\gamma_i, \gamma_j) \quad (i<j),$$

and

$$a\left(\prod_{i=1}^{m} \gamma_i^{t_i}, \prod_{i=1}^{m} \gamma_i^{q_i}\right) = \prod_{i=1}^{m} a(\gamma_i, \gamma_i^{-1})^{o_i(t_i, q_i)} \prod_{i<j} a(\gamma_j, \gamma_i)^{q_i t_j}. \tag{2·9}$$

Conversely, every factor system satisfying (2·9) can be given in form (2·8). On the other hand, the elements $a \in F(\Gamma, \Delta)$ satisfying (2·9) form a subgroup $F_{\mathfrak{g}}(\Gamma, \Delta)$. We conclude that the mapping $a \rightarrow \bar{a}$ induces a homomorphism of $F_{\mathfrak{g}}(\Gamma, \Delta)$ *onto* $\bar{F}(\Gamma, \Delta)$, and if Δ is of finite exponent d, and $d \mid n_i$, for $i = 1, \ldots, m$, then this homomorphism is an isomorphism. If we make this additional hypothesis on Δ we thus get for every given basis an explicit representation of $\bar{F}(\Gamma, \Delta)$ by a group $F_{\mathfrak{g}}(\Gamma, \Delta)$ of factor systems.

3. The exact sequence describing $\mathfrak{C}(\mathrm{K}/\mathrm{P})$

Notation. K is an Abelian extension field of a field P, of characteristic zero. The degree (K: P) is some power of a prime l. $\mathfrak{C}(\mathrm{K}/\mathrm{P})$ is the set of all cyclic extensions Λ of K, whose relative degree over K is a divisor of l, and which are normal over P. $\bar{\Lambda} = \bar{\Lambda}(\mathrm{K})$ is the union of the fields in $\mathfrak{C}(\mathrm{K}/\mathrm{P})$. We write for briefness $\Gamma = \Gamma(\mathrm{K}/\mathrm{P})$, $\bar{\Gamma} = \Gamma(\bar{\Lambda}/\mathrm{P})$, and if M is a field between K and $\bar{\Lambda}$, $\Gamma_{\mathrm{M}} = \Gamma(\bar{\Lambda}/\mathrm{M})$. E is the group of complex lth roots of unity. We note that every field Λ in $\mathfrak{C}(\mathrm{K}/\mathrm{P})$ is a central extension of K over P, whence the same is true for every field M between K and $\bar{\Lambda}$. The theory of § 2 thus applies here.

With the set $\mathfrak{C}(\mathrm{K}/\mathrm{P})$ there are associated as description invariants four groups connected by certain mappings. These are the character groups (i) $\Phi(\mathrm{K}/\mathrm{P})$, (ii) $\Phi(\bar{\Lambda}/\mathrm{K})$, (iii) the subgroup $\Psi(\mathrm{K}/\mathrm{P})$ of $\Phi(\mathrm{P})$ generated by $\Phi(\mathrm{K}/\mathrm{P})$ and by all characters of order l, and (iv) a subgroup $A(\mathrm{K}/\mathrm{P}) = A(\mathrm{K})$ of $\bar{F}(\Gamma, E)$ presently to be defined.

† $a^*(\gamma) \bmod \Delta^{n_\gamma}$ is, however, not determined by the values $a^*(\gamma_i)$ only; we need also the values $a_*(\gamma_i, \gamma_j)$.

‡ Throughout this paper $\prod_{i<j}$ is the product over all pairs (i, j) with $1 \leqslant i < j \leqslant m$.

$\Phi(\mathrm{K/P})$ is a subgroup of $\Psi(\mathrm{K/P})$; we denote the injection mapping of $\Phi(\mathrm{K/P})$ into $\Psi(\mathrm{K/P})$ by $I_{\mathrm{K/P}}$. Next we observe that the union $\overline{\mathrm{K}}$ of K and of all cyclic extensions of P of degree l is a subfield of $\overline{\Lambda}$, and that $\Psi(\mathrm{K/P}) = \Phi(\overline{\mathrm{K}}/\mathrm{P})$. It follows that $R_{\mathrm{P/K}}$ maps $\Psi(\mathrm{K/P})$ into $\Phi(\overline{\Lambda}/\mathrm{K})$; the same symbol $R_{\mathrm{P/K}}$ will be used for this induced mapping.

Choose a representative $a \in F(\Gamma, \Gamma_{\mathrm{K}})$ of the operative class $\bar{a}(\mathrm{K})$ for $\overline{\Lambda}/\mathrm{K/P}$, and write for all $\phi \in \Phi(\overline{\Lambda}/\mathrm{K})$ and for all $\gamma_1, \gamma_2 \in \Gamma$

$$c_{a,\phi}(\gamma_1, \gamma_2) = \phi(a(\gamma_1, \gamma_2)). \tag{3·1}$$

Then $c_{a,\phi} \in F(\Gamma, E)$ for each $\phi \in \Phi(\overline{\Lambda}/\mathrm{K})$, and the class $\bar{c}_{a,\phi}$ does not depend on a but solely on $\bar{a}(\mathrm{K})$, i.e. on K, and on ϕ. Put

$$u_{\mathrm{K/P}}\,\phi = \bar{c}_{a,\phi}. \tag{3·2}$$

$u_{\mathrm{K/P}}$ is a homomorphism of $\Phi(\overline{\Lambda}/\mathrm{K})$ into $\overline{F}(\Gamma, E)$, whose image group is the group $A(\mathrm{K/P})$. We then have

THEOREM 1. *The sequence of homomorphisms*

$$S_{\mathrm{K/P}}:\quad 1 \longrightarrow \Phi(\mathrm{K/P}) \xrightarrow{I_{\mathrm{K/P}}} \Psi(\mathrm{K/P}) \xrightarrow{R_{\mathrm{P/K}}} \Phi(\overline{\Lambda}/\mathrm{K}) \xrightarrow{u_{\mathrm{K/P}}} A(\mathrm{K/P}) \longrightarrow 1$$

is exact.

Proof.† I is clearly an isomorphism into $\Psi(\mathrm{K/P})$. Next observe that if $\psi \in \Psi(\mathrm{K/P}) = \Phi(\overline{\mathrm{K}}/\mathrm{P})$, and if $\phi = R\psi$, then for all $\gamma \in \Gamma_{\mathrm{K}}$, $\phi(\gamma) = \psi(\gamma\Gamma_{\overline{\mathrm{K}}})$. Hence $\phi(\gamma) = 1$, for all $\gamma \in \Gamma_{\mathrm{K}}$, if and only if $\psi(\bar{\gamma}) = 1$, for all $\bar{\gamma} \in \Gamma(\overline{\mathrm{K}}/\mathrm{K}) = \Gamma_{\mathrm{K}}/\Gamma_{\overline{\mathrm{K}}}$. It follows that $\phi = 1$, if and only if $\psi \in \Phi(\mathrm{K/P})$, so that the kernel of R is the image of I.

Let now $\phi \in \Phi(\overline{\Lambda}/\mathrm{K})$ and put $\Lambda = \mathrm{K}_\phi$. If $\Lambda = \mathrm{KK}'$ where K' is cyclic over P, and $(\mathrm{K}' : \mathrm{P})$ divides l, then $\mathrm{K}' = \mathrm{P}_\psi$, with $\psi \in \Psi(\mathrm{K/P})$, and $\phi = R\psi^r$. Conversely, if $\phi = R\psi$, with $\psi \in \Psi(\mathrm{K/P})$, then one can assume $\psi^l = 1$, and thus $\mathrm{P}_\psi = \mathrm{K}'$, $\Lambda = \mathrm{KK}'$ where K' is cyclic over P, and $(\mathrm{K}' : \mathrm{P})$ divides l.

Choose a representative a in $F(\Gamma, \Gamma_{\mathrm{K}})$ of $\bar{a}(\mathrm{K})$, and write $d(\gamma_1, \gamma_2) = a(\gamma_1, \gamma_2)\,\Gamma_\Lambda$ for all $\gamma_1, \gamma_2 \in \Gamma$. Then $d \in F(\Gamma, \Gamma(\Lambda/\mathrm{K}))$, and $\bar{d}$ is independent of the particular choice of a. Furthermore, $\bar{d}$ is the operative class for $\Lambda/\mathrm{K/P}$. The function ϕd defined by

$$\phi d(\gamma_1, \gamma_2) = \phi(d(\gamma_1, \gamma_2))$$

for all $\gamma_1, \gamma_2 \in \Gamma$, lies in $F(\Gamma, E)$, and $\overline{\phi d} = u\phi$. Observing that ϕ is an isomorphism of $\Gamma(\Lambda/\mathrm{K})$ into E, we conclude that $u\phi = 1$, if and only if $\bar{d} = 1$, i.e. if and only if $\Lambda = \mathrm{KK}'$, where K' is cyclic over P and $(\mathrm{K}' : \mathrm{P})$ divides l. Thus $u\phi = 1$, if and only if $\phi \in R\Psi(\mathrm{K/P})$. This completes the proof of theorem 1.

A few remarks on the determination of the operative class $\bar{d}_\Lambda$ for $\Lambda/\mathrm{K/P}$ and of its type, by $u\phi$ may be useful. If ϕ generates $\Phi(\Lambda/\mathrm{K})$, and if $c \in F(\Gamma, E)$ is a representative of $u\phi$, the equations

$$c(\gamma_1, \gamma_2) = \phi(d(\gamma_1, \gamma_2)) \tag{3·3}$$

determine a representative d of $\bar{d}_\Lambda$. On the other hand, if we take c merely as a representative of a generator of the group $A_\Lambda = u\Phi(\Lambda/\mathrm{K})$ we still retain the equation $\bar{c} = (u\phi)^r$ for some r prime to l. In this case the element d defined by (3·3) will satisfy the relation $\bar{d} = \bar{d}_\Lambda^r$. It follows easily that the types of $\bar{d}$ and $\bar{d}_\Lambda$ coincide. Thus the group A_Λ itself uniquely determines the operative type for $\Lambda/\mathrm{K/P}$. But every element of $A(\mathrm{K})$ generates a group A_Λ,

† From now on we write $R = R_{\mathrm{P/K}}$, $I = I_{\mathrm{K/P}}$, $u = u_{\mathrm{K/P}}$, etc., except when there is danger of confusion.

and conversely always $A_{\Lambda} \subseteq A(\mathrm{K})$. Thus the group $A(\mathrm{K})$ can be characterized as the subgroup of $\overline{F}(\Gamma, E)$ of classes which represent operative types for $\Lambda/\mathrm{K}/\mathrm{P}$ as Λ varies over $\mathfrak{C}(\mathrm{K}/\mathrm{P})$.

We note here that if M is a union of some fields in $\mathfrak{C}(\mathrm{K}/\mathrm{P})$, then the exact sequence in theorem 1 characterizes the operative factor-system class, and the operative type of $\mathrm{M}/\mathrm{K}/\mathrm{P}$ in the same way as when in particular $\mathrm{M} \in \mathfrak{C}(\mathrm{K}/\mathrm{P})$. For, choosing a set of representatives of Γ, and denoting by c_{ϕ} the corresponding representative of $u\phi$ in $F(\Gamma, E)$, the equations $c_{\phi}(\gamma, \gamma') = \phi(d(\gamma, \gamma'))$, for all $\gamma, \gamma' \in \Gamma$, and for all $\phi \in \Phi(\mathrm{M}/\mathrm{K})$, will determine the unique factor system d in $F(\Gamma, \Gamma(\mathrm{M}/\mathrm{K}))$, and $\bar{d}$ is the operative class for $\mathrm{M}/\mathrm{K}/\mathrm{P}$. One can in fact easily derive from the theory of $\mathfrak{C}(\mathrm{K}/\mathrm{P})$ a theory of the set of fields M such that (i) M is composed of cyclic extensions of K of relative degree l, (ii) M is a central extension of K over P. Every such field is then composed of fields in $\mathfrak{C}(\mathrm{K}/\mathrm{P})$ and the results on these fields are easily extended. We shall, however, not explicitly refer again to this question.

The notation for the invariants of $\mathfrak{C}(\mathrm{K}/\mathrm{P})$ and their homomorphisms will be used throughout this paper.

Assume now that P is either a finite algebraic number field or a finite algebraic extension of a completion of the rational field for some valuation. Denote by V the multiplicative group of P, and if P is an algebraic number field by J the idèle group of P. If P is an algebraic number field we consider† the factor systems c of J in E, satisfying for all $\mathfrak{a}, \mathfrak{b} \in J$

$$c(\mathfrak{a}, \mathfrak{b}) = 1, \quad \text{if either} \quad \phi(\mathfrak{a}) = 1 \quad \text{or} \quad \phi(\mathfrak{b}) = 1, \quad \text{for all } \phi \in \Phi(\mathrm{K}/\mathrm{P}). \tag{3·4}$$

From (3·4) we easily conclude that $c(\mathfrak{a}, \mathfrak{b})$ solely depends on the values $\phi(\mathfrak{a})$, $\phi(\mathfrak{b})$ for all $\phi \in \Phi(\mathrm{K}/\mathrm{P})$. If, on the other hand, P is a $\mathfrak{p}$-adic field, we consider the factor systems c satisfying (3·4) for all $\mathfrak{a}, \mathfrak{b} \in V$. In both cases these factor systems form a group which will be denoted by $F(H(\mathrm{K}), E)$; our notation indicates that this is essentially the group of factor systems in E of the class group $H(\mathrm{K})$. Denote the Artin mapping of J, respectively, V onto Γ by g, i.e. g is the mapping $\mathfrak{a} \to (\mathrm{K}/\mathrm{P}; \mathfrak{a})$. Then if $a \in F(\Gamma, E)$, the function g^*a defined by

$$g^*a(\mathfrak{a}, \mathfrak{b}) = a(g\mathfrak{a}, g\mathfrak{b})$$

is an element of $F(H(\mathrm{K}), E)$. The mapping g^* is an isomorphism onto $F(H(\mathrm{K}), E)$, and the class $\overline{g^*a}$ solely depends on $\bar{a}$. We put $\overline{g^*a} = \bar{g}\bar{a}$; then g is a canonical isomorphism of $\overline{F}(\Gamma, E)$ onto $\overline{F}(H(\mathrm{K}), E)$. We shall in future identify the groups $F(H(\mathrm{K}), E)$ and $\overline{F}(H(\mathrm{K}), E)$ with $F(\Gamma, E)$ and $\overline{F}(\Gamma, E)$, respectively.

4. Class group interpretation

In this section it will be assumed that P is a finite algebraic number field, or a finite algebraic extension of a local completion of the rational field. A characterization of the groups $\Phi(\overline{\Lambda}/\mathrm{K})$, $A(\mathrm{K})$, and of the mappings R and u in terms of class groups in K will be derived. Together with the corresponding characterization of the groups $\Phi(\mathrm{K}/\mathrm{P})$, $\Psi(\mathrm{K}/\mathrm{P})$ in P, which follows immediately as in § 1, by Artin's law of reciprocity, this provides the definitions in § 1 (and § 6), and the statement of theorem 1 (and 4) with a meaning in terms of class-field theory over K, and makes it possible to interpret the results obtained in §§ 7

† It would be of interest to consider the group of all factor systems c, for which (3·4) is satisfied not with the group $\Phi(\mathrm{K}/\mathrm{P})$, but with an arbitary finite subgroup Φc of $\Phi(\mathrm{P})$. It is hoped to return to this question.

to 12 as determining by criteria in P properties of class groups in K. This interpretation is an application to a special case of known results of class-field theory (see, for example, Chevalley 1954).

The following notation will be used. For any finite algebraic number field M, J_M is the idèle group, and V_M is the multiplicative group of M. $N_{M/M'}$ is the norm operator, when M′ is a subfield of M. If $\gamma \in \Gamma$, K_γ is the invariant field of the cyclic group $\{\gamma\}$ in Γ. L_K is the group of idèles $\mathfrak{A}$ in J_K for which $N_{K/P}\,\mathfrak{A}$ lies in $J_P^l V_P$. M_K is the group of idèles $\mathfrak{A}$ in J_K of form

$$\mathfrak{A} = \alpha\mathfrak{A}_1^l . \prod_\gamma (\gamma\mathfrak{B}_\gamma . \mathfrak{B}_\gamma^{-1}),$$

where the product extends over all $\gamma \in \Gamma$, and where $\mathfrak{A}_1, \mathfrak{B}_\gamma \in J_K$, $\alpha \in V_K$. Clearly $M_K \subseteq L_K$.

We shall restrict ourselves to finite algebraic number fields. If P is instead taken as a 'local' field both results and proofs apply with the appropriate changes in notation; one only has to replace throughout 'idèles' by 'non-zero elements of the field', and substitute the multiplicative group V_M for the idèle group J_M, and the group of order 1 for the multiplicative group V_M in all formulae.

Let $\Phi(M_K)$ be the group of characters λ of M_K which are restrictions of idèle class characters to M_K, i.e. such that $\exists\phi \in \Phi(K)$ with $\phi(\mathfrak{A}) = \lambda(\mathfrak{A})$, for all $\mathfrak{A} \in M_K$. Denote here the restriction of a character ϕ in $\Phi(K)$ to M_K by $r_M\phi$; thus r_M is a homomorphism of $\Phi(K)$ onto $\Phi(M_K)$. Let furthermore $\Phi(L_K/M_K)$ be the group of characters λ of L_K, such that, first, $\exists\phi \in \Phi(K)$ with $\phi(\mathfrak{A}) = \lambda(\mathfrak{A})$, for all $\mathfrak{A} \in L_K$, and that, secondly, $\lambda(\mathfrak{A}) = 1$, if $\mathfrak{A} \in M_K$. Denote the restriction of a character $\phi \in \Phi(\bar{\Lambda}/K)$ to L_K by r_L and the restriction of a character ϕ in $\Phi(P)$ to the norms of K in P by s; the characters $s\phi$ form a group $\Phi(N_{K/P}\,J_K)$.

One may, without loss of generality assume that $K \neq P$. The exponent of E then divides the order of all non-unit elements of Γ. Under this hypothesis, however, it was proved in §2 that for any factor system c in $F(\Gamma, E)$, the power factors $c^*(\gamma)$ and the commutator factors $c_*(\gamma, \delta)$, for all $\gamma, \delta \in \Gamma$ depend solely on the class $\bar{c}$ of c, and in turn uniquely determine this class. This trivially remains true if $K = P$. A characterization of $u\phi = \bar{c}$ will then be given in terms of the factors $c^*(\gamma)$, $c_*(\gamma, \delta)$.

Theorem 2. *Let* P *be a finite algebraic number field*

(i) *If* $\phi \in \Phi(P)$, *and* $\mathfrak{A} \in J_K$, *then*

$$[R\phi]\,(\mathfrak{A}) = \phi(N_{K/P}\mathfrak{A}). \tag{4·1}$$

The sequence† *of homomorphisms*

$$T_1\colon\quad 1 \to \Phi(K/P) \to \Phi(P) \xrightarrow{s} \Phi(N_{K/P}\,J_K) \to 1$$

is exact. The mapping $s\psi \to R\psi$, *for all* $\psi \in \Psi(K/P)$ *sets up a canonical isomorphism of* $\Psi(K/P)/\Phi(K/P)$ *onto* $R\Psi(K/P)$ *in accordance with* (4·1).

(ii) *A character* ϕ *in* $\Phi(K)$ *will lie in* $\Phi(\bar{\Lambda}/K)$ *if and only if*

$$\phi(\mathfrak{A}^l) = \phi(\gamma\mathfrak{A} . \mathfrak{A}^{-1}) = 1 \tag{4·2}$$

for all $\mathfrak{A} \in J_K$, *and all* $\gamma \in \Gamma$. $\Phi(\bar{\Lambda}/K)$ *is thus the subgroup of* $\Phi(K)$ *of characters taking value* 1 *on* M_K. *The sequence of homomorphisms*

$$T_2\colon\quad 1 \to \Phi(\bar{\Lambda}/K) \to \Phi(K) \xrightarrow{r_M} \Phi(M_K) \to 1$$

is exact.

† The mapping $\Phi(K/P) \to \Phi(P)$ in T_1 is the injection mapping, and the same is true for the second homomorphisms in T_2, T_3.

(iii) *Let γ, δ be any two given elements of* Γ. *Then there exist* $\mathfrak{a} \in J_{K_\gamma}$, $\alpha \in V_{K_\gamma}$, *and* $\mathfrak{A}_\gamma, \mathfrak{B}_{\delta,\gamma} \in J_K$ *such that*

$$(K/K_\gamma; \mathfrak{a}) = \gamma, \tag{4·3}$$

$$N_{K/K_\gamma}\mathfrak{A}_\gamma = \mathfrak{a}^{n_\gamma}, \quad n_\gamma = \text{order}\,\gamma, \tag{4·4}$$

$$N_{K/K_\gamma}\mathfrak{B}_{\delta,\gamma} = \delta\mathfrak{a}\,.\,\mathfrak{a}^{-1}.\alpha. \tag{4·5}$$

Let $$\phi \in \Phi(\overline{\Lambda}/K), \quad u\phi = \bar{c}.$$

Then for all $\mathfrak{A}_\gamma$ *satisfying* (4·4), (4·3) *for some* $\mathfrak{a} \in J_{K_\gamma}$

$$\phi(\mathfrak{A}_\gamma) = c^*(\gamma) \tag{4·6}$$

provided that $\gamma \neq 1$, *and for all* $\mathfrak{B}_{\delta,\gamma}$ *satisfying* (4·5), (4·3) *with some* $\mathfrak{a} \in J_{K_\gamma}$

$$\phi(\mathfrak{B}_{\delta,\gamma}) = c_*(\delta, \gamma). \tag{4·7}$$

For all $\phi \in \Phi(\overline{\Lambda}/K)$, *and all* $\gamma, \delta \in \Gamma$ *there exist idèles* $\mathfrak{A}_\gamma$, $\mathfrak{B}_{\delta,\gamma}$ *in* L_K *satisfying* (4·6), (4·7). *For all* $\phi \in \Phi(\overline{\Lambda}/K)$, $r_L\phi$ *lies in* $\Phi(L_K/M_K)$, *and the sequence of homomorphisms*

$$T_3\colon \quad 1 \to R\Psi(K/P) \to \Phi(\overline{\Lambda}/K) \xrightarrow{r_L} \Phi(L_K/M_K) \to 1$$

is exact. The mapping $r_L\phi \to u\phi = \bar{c}$, *set up by* (4·6), (4·7) *if* $\mathfrak{A}_\gamma, \mathfrak{B}_{\delta,\gamma} \in L_K$, *for all* $\gamma, \delta \in \Gamma$ *is an isomorphism of* $\Phi(L_K/M_K)$ *onto* $A(K)$.

Theorem 2 thus characterizes $\Phi(\overline{\Lambda}/K)$ by (4·2) as indicated, and $A(K)$ essentially as the group $\Phi(L_K/M_K)$ of restricted idèle class characters. The interpretation of the mappings R and u is given in (4·1), and in (4·3) to (4·7), respectively.

Proof. (4·1) follows by the norm formula for Artin symbols:

$$((\Lambda/K; \mathfrak{A}) = (\Lambda/P; N_{K/P}\mathfrak{A}) \quad \text{if} \quad \Lambda = K_{\phi'}, \phi' = R\phi).$$

The remainder of (i) follows by the interpretation of $\Phi(K/P)$ as a group of idèle class characters (cf. §1), and by the fundamental theorem of class-field theory (cf. Chevalley 1940).

For (ii) we observe that if $\phi \in \Phi(\overline{\Lambda}/K)$, $\Lambda = K_\phi$ then Λ is a central extension of K over P, and $(\Lambda : K)$ divides l. Therefore for all $\mathfrak{A} \in J_K$, all $\gamma \in \Gamma$

$$(\Lambda/K; \mathfrak{A}^l) = (\Lambda/K; \gamma\mathfrak{A}\,.\,\mathfrak{A}^{-1}) = 1,$$

and so ϕ satisfies (4·2). Conversely, if (4·2) holds, then—for $K_\phi = \Lambda$—so do the equations on Artin symbols given here, and so Λ is normal over P, and $(\Lambda : K)$ divides l, i.e. $\Lambda \in \mathfrak{C}(K/P)$, $\phi \in \Phi(\overline{\Lambda}/K)$. The rest of (ii) follows from this characterization of $\Phi(\overline{\Lambda}/K)$. We note that as a consequence $r_L\phi \in \Phi(L_K/M_K)$, for all $\phi \in \Phi(\overline{\Lambda}/K)$, so that r_L is certainly a homomorphism into $\Phi(L_K/M_K)$.

To establish (iii) we choose for given $\phi \in \Phi(\overline{\Lambda}/K)$, a factor system a in the operative class of $K_\phi/K/P$. If $\gamma, \delta \in \Gamma$, $\gamma \neq 1$, and if $\bar{\gamma}, \bar{\delta}$ are any representatives of these elements in $\Gamma(K_\phi/P)$, then we have for the commutator $(\bar{\delta}, \bar{\gamma}) = \bar{\delta}^{-1}\bar{\gamma}^{-1}\bar{\delta}\bar{\gamma}$ the formula

$$(\bar{\delta}, \bar{\gamma}) = a_*(\delta, \gamma), \tag{4·8}$$

and for $\bar{\gamma}^{n_\gamma}$—where n_γ is the order of γ—the formula

$$\bar{\gamma}^{n_\gamma} = a^*(\gamma). \tag{4·9}$$

Now let $\mathfrak{p}$ be a finite prime divisor in P, non-ramified in K, such that $(\mathrm{K/P}; \mathfrak{p}) = \gamma$. Such a prime divisor will always exist. Any prime divisor $\mathfrak{P}$ in K_γ lying above $\mathfrak{p}$ satisfies $(\mathrm{K/K}_\gamma; \mathfrak{P}) = \gamma$. Let $\mathfrak{a}$ be an idèle in K_γ which is of order 1 at $\mathfrak{P}$, and has local components $\mathfrak{a}_\mathfrak{Q} = 1$, for all prime divisors $\mathfrak{Q}$ in K_γ distinct from $\mathfrak{P}$. Then $\mathfrak{a}$ satisfies (4·3), and $\mathfrak{A}_\gamma = \mathfrak{a}$ satisfies (4·4). Also if $\delta \in \Gamma$, $(\mathrm{K/K}_\gamma; \delta\mathfrak{a}.\mathfrak{a}^{-1}) = 1$, and so for some $\alpha \in V_{\mathrm{K}\gamma}$, $\mathfrak{B}_{\delta,\gamma} \in J_{\mathrm{K}}$ (4·5) will hold.

Assume now that $\mathfrak{A}_\gamma$ satisfies (4·4), (4·3). As K_ϕ is a central extension of K over P, and as $\mathrm{K/K}_\gamma$ is cyclic, K_ϕ is an Abelian extension of K_γ. There thus exists a representative $\bar{\gamma}$ of γ in $\Gamma(\mathrm{K}_\phi/\mathrm{K}_\gamma)$ such that $(\mathrm{K}_\phi/\mathrm{K}_\gamma; \mathfrak{a}) = \bar{\gamma}$. Then $(\mathrm{K}_\phi/\mathrm{K}; \mathfrak{A}_\gamma) = (\mathrm{K}_\phi/\mathrm{K}_\gamma; \mathfrak{a}^{n_\gamma})$ and so

$$(\mathrm{K}_\phi/\mathrm{K}; \mathfrak{A}_\gamma) = \bar{\gamma}^{n_\gamma}. \tag{4·10}$$

Assume that $\mathfrak{B}_{\delta,\gamma}$ satisfies (4·5), (4·3). As before we get $(\mathrm{K}_\phi/\mathrm{K}_\gamma; \mathfrak{a}\alpha) = (\mathrm{K}_\phi/\mathrm{K}_\gamma; \mathfrak{a}) = \bar{\gamma}$ and hence $(\mathrm{K}_\phi/\mathrm{K}_\gamma; \delta\mathfrak{a}.\mathfrak{a}^{-1}.\alpha) = (\bar{\delta}, \bar{\gamma})$. Thus

$$(\mathrm{K}_\phi/\mathrm{K}; \mathfrak{B}_{\delta,\gamma}) = (\bar{\delta}, \bar{\gamma}). \tag{4·11}$$

Finally, using $\phi(a_*(\delta,\gamma)) = c_*(\delta,\gamma)$, $\phi(a^*(\gamma)) = c^*(\gamma)$ when $\bar{c} = u\phi$, (4·6), (4·7) follow by (4·8) to (4·11).

We have seen that (4·3) to (4·5) implies (4·6), (4·7). Also the existence of idèles satisfying (4·3) to (4·5) has been established. But any such idèles will lie in L_{K}, and so there exist for all $\phi \in \Phi(\bar{\Lambda}/\mathrm{K})$, and for all $\gamma, \delta \in \Gamma$ idèles in L_{K} satisfying (4·6), (4·7). The case $\gamma = 1$, which was excluded, is trivial.

We have already seen that r_L is a homomorphism into $\Phi(L_{\mathrm{K}}/M_{\mathrm{K}})$. Assume now that $\lambda \in \Phi(L_{\mathrm{K}}/M_{\mathrm{K}})$. Then $\lambda = r_L\phi$, for some $\phi \in \Phi(\mathrm{K})$. But $\lambda(\mathfrak{A}) = 1$ if $\mathfrak{A} \in M_{\mathrm{K}}$. Also $M_{\mathrm{K}} \subseteq L_{\mathrm{K}}$. Therefore $\phi(\mathfrak{A}) = 1$ if $\mathfrak{A} \in M_{\mathrm{K}}$, and hence by (ii) $\phi \in \Phi(\bar{\Lambda}/\mathrm{K})$. Thus r_L is a homomorphism of $\Phi(\bar{\Lambda}/\mathrm{K})$ onto $\Phi(L_{\mathrm{K}}/M_{\mathrm{K}})$.

Let $\psi \in \Psi(\mathrm{K/P})$ and $\mathfrak{A} \in L_{\mathrm{K}}$. Then $N_{\mathrm{K/P}}\mathfrak{A} \in J^l_{\mathrm{P}} V_{\mathrm{P}} \cap N_{\mathrm{K/P}} J_{\mathrm{K}}$, and so $\psi(N_{\mathrm{K/P}}\mathfrak{A}) = 1$, hence by (4·1) $[R\psi](\mathfrak{A}) = 1$. Thus $R\Psi(\mathrm{K/P})$ lies in the kernel of r_L in $\Phi(\bar{\Lambda}/\mathrm{K})$. Conversely, assume that for $\phi \in \Phi(\bar{\Lambda}/\mathrm{K})$, $r_L\phi = 1$. If then the idèles $\mathfrak{B}_{\delta,\gamma}$, $\mathfrak{A}_\gamma$ $(\gamma \neq 1)$ satisfy (4·3) to (4·5) they will lie in L_{K}, and hence

$$\phi(\mathfrak{A}_\gamma) = \phi(\mathfrak{B}_{\delta,\gamma}) = 1.$$

But $\mathfrak{A}_\gamma$ satisfies (4·6), $\mathfrak{B}_{\gamma,\delta}$ satisfies (4·7). Hence for $\bar{c} = u\phi$ we get $c^*(\gamma) = c_*(\gamma,\delta) = 1$ and this is true for all $\gamma, \delta \in \Gamma$. Thus $u\phi = 1$, and hence by theorem 1 $\phi \in R\Psi(\mathrm{K/P})$. Thus T_3 is exact; this, however, implies that the mapping $r_L\phi \to u\phi$ defines an isomorphism of $\Phi(L_{\mathrm{K}}/M_{\mathrm{K}})$ onto $A(\mathrm{K})$.

5. Kummer interpretation

In the present section a special situation will be considered. It will be assumed—in this section only—that P is a field of characteristic zero (or of characteristic prime to l) containing the primitive lth roots of unity, and an interpretation of the invariants associated with $\mathfrak{C}(\mathrm{K/P})$ in terms of 'Kummer' invariants will be derived. Whenever the hypothesis made here applies, the results of §§ 7 to 12 can then be interpreted as providing a rational determination of certain Kummer invariants in K. Apart from this, the subject matter of this section has no direct bearing on the rest of the paper, and will not be used elsewhere.†

† The interpretation of invariants in which we are mainly interested is that discussed in §4.

We shall not discuss all aspects of the 'Kummer interpretation' in detail. A detailed treatment of this problem for relatively Abelian extensions in general has—from a slightly different point of view—been given in Hasse (1947).

Denote the multiplicative group of a field M containing P again by V_{M}; if M′ is an extension field denote the subgroup of $V_{\mathrm{M}'}$ of elements whose lth powers lie in M by $W(\mathrm{M}'/\mathrm{M})$. Throughout this section, whenever W is a subgroup of the group V_{M} for some field M, and Ω is a Galois group of M over some subfield, the operation of Ω on W is supposed to be induced by the operation of Ω as Galois group of M. Homomorphisms are taken as operator homomorphisms, and the groups $F(\Omega, W)$, $\bar{F}(\Omega, W)$ are defined with respect to the given realization of Ω by automorphisms of W—which, in this section, need not be the trivial one.

If E' is the group of lth roots of unity, the group Γ will leave E' as a subgroup of V_{P} element-wise fixed. We can thus identify E' with E, and take over without change the definitions and results of § 3.†

Assume again that the field M contains P, and so contains E. If M′ is an Abelian extension of M, then we define for all $\mathrm{A} \in W(\mathrm{M}'/\mathrm{M})$ a function θ_{A} on $\Gamma(\mathrm{M}'/\mathrm{M})$ by

$$\theta_{\mathrm{A}}(\gamma) = \gamma\mathrm{A}\,.\,\mathrm{A}^{-1}, \quad \text{for all} \quad \gamma \in \Gamma(\mathrm{M}'/\mathrm{M}). \tag{5·1}$$

θ_{A} is a character in $\Phi(\mathrm{M}'/\mathrm{M})$. Denoting the subgroup of characters ϕ in $\Phi(\mathrm{M}'/\mathrm{M})$ with $\phi^l = 1$ by $\Phi_{(l)}(\mathrm{M}'/\mathrm{M})$, we verify easily that the mapping $\mathrm{A} \rightarrow \theta_{\mathrm{A}}$ is a homomorphism of $W(\mathrm{M}'/\mathrm{M})$ onto $\Phi_{(l)}(\mathrm{M}'/\mathrm{M})$ with kernel V_{M}.‡ We denote the isomorphism of $W(\mathrm{M}'/\mathrm{M})/V_{\mathrm{M}}$ onto $\Phi_{(l)}(\mathrm{M}'/\mathrm{M})$ induced by the mapping $\mathrm{A} \rightarrow \theta_{\mathrm{A}}$ by $z_{\mathrm{M}'/\mathrm{M}}$.

The group $W(\mathrm{K}/\mathrm{P})/V_{\mathrm{P}}$ is a subgroup of $W(\bar{\mathrm{K}}/\mathrm{P})/V_{\mathrm{P}}$; denote the injection mapping by I'. Also $W(\bar{\mathrm{K}}/\mathrm{P}) \subseteq W(\bar{\Lambda}/\mathrm{K})$; hence the mapping $\mathrm{A}V_{\mathrm{P}} \rightarrow \mathrm{A}V_{\mathrm{K}}$, for all $\mathrm{A} \in W(\bar{\mathrm{K}}/\mathrm{P})$ defines a homomorphism of $W(\bar{\mathrm{K}}/\mathrm{P})/V_{\mathrm{P}}$ into $W(\bar{\Lambda}/\mathrm{K})/V_{\mathrm{K}}$, to be denoted by R'.

Next let $\mathrm{A} \in W(\bar{\Lambda}/\mathrm{K})$, and let Γ' be a complete set of representatives of Γ in $\bar{\Gamma}$; we denote the representative of γ by $\bar{\gamma}$. The field K(A) is a cyclic extension of K and a subfield of $\bar{\Lambda}$ and hence lies in $\mathfrak{C}(\mathrm{K}/\mathrm{P})$. K(A) is thus a central extension of K over P. It follows that if $\gamma \in \Gamma$, then $\exists b(\gamma) \in V_{\mathrm{K}}$ with

$$\bar{\gamma}\mathrm{A} = b(\gamma)\,\mathrm{A}. \tag{5·2}$$

By direct calculation we then obtain for all $\gamma, \delta \in \Gamma$

$$\overline{\gamma\delta}^{-1}\bar{\gamma}\bar{\delta}\mathrm{A} = c_{\mathrm{A}}(\gamma, \delta)\,\mathrm{A}, \tag{5·3}$$

where

$$c_{\mathrm{A}}(\gamma, \delta) \in E \tag{5·4}$$

as $\overline{\gamma\delta}^{-1}\bar{\gamma}\bar{\delta} \in \Gamma_{\mathrm{K}}$. Also, as $E \subseteq V_{\mathrm{P}}$, we have $\gamma\delta c_{\mathrm{A}}(\gamma, \delta) = c_{\mathrm{A}}(\gamma, \delta)$, and so

$$c_{\mathrm{A}}(\gamma, \delta) = b(\gamma)\,.\,\gamma b(\delta)\,.\,(b(\gamma\delta))^{-1}. \tag{5·5}$$

It follows by (5·4), (5·5) that $c_{\mathrm{A}} \in F(\Gamma, E)$. Replacing A by $\mathrm{A}\beta, \beta \in V_{\mathrm{K}}$, will not affect c_{A}, and replacing Γ' by another set of representatives will not affect $\bar{c}_{\mathrm{A}}$. Thus $\bar{c}_{\mathrm{A}}$ solely depends on the coset $\mathrm{A}V_{\mathrm{K}}$. The mapping $\mathrm{A}V_{\mathrm{K}} \rightarrow \bar{c}_{\mathrm{A}}$ thus defines a homomorphism of $W(\bar{\Lambda}/\mathrm{K})/V_{\mathrm{K}}$ into $\bar{F}(\Gamma, E)$, denoted by u'.

† We note in particular that the 'new' definition of $\bar{F}(\Gamma, E)$ coincides with the 'old' one, and that this convention leaves the types in $\bar{F}(\Gamma, E)$ invariant, as pointed out in §2.

‡ For proofs of these results when M′/M is finite see, for example, Hasse (1947). The proofs immediately extend to the infinite case.

Observe now that $F(\Gamma, E)$ is a subgroup of $F(\Gamma, V_{\mathrm{K}})$. The class in $\overline{F}(\Gamma, V_{\mathrm{K}})$ of an element of $F(\Gamma, E)$ solely depends on its class in $\overline{F}(\Gamma, E)$. The mapping of the classes in $\overline{F}(\Gamma, E)$ onto the classes in $\overline{F}(\Gamma, V_{\mathrm{K}})$ of their representatives in $F(\Gamma, E)$ is a homomorphism which will here be denoted by y. Finally, denote the injection mapping of $A(\mathrm{K})$ in $\overline{F}(\Gamma, E)$ by x. Then we have

THEOREM 3. (i) *The image group of u' is $A(\mathrm{K})$, and the sequence*

$$S'\colon\quad 1 \rightarrow W(\mathrm{K}/\mathrm{P})/V_{\mathrm{P}} \xrightarrow{I'} W(\overline{\mathrm{K}}/\mathrm{P})/V_{\mathrm{P}} \xrightarrow{R'} W(\overline{\Lambda}/\mathrm{K})/V_{\mathrm{K}} \xrightarrow{u'} A(\mathrm{K}) \rightarrow 1$$

is exact. Also the sequence

$$T\colon\quad A(\mathrm{K}) \xrightarrow{x} \overline{F}(\Gamma, E) \xrightarrow{y} \overline{F}(\Gamma, V_{\mathrm{K}})$$

is exact.

(ii) *The diagram*[†]

$$\begin{tikzcd}
W(\mathrm{K}/\mathrm{P})/V_{\mathrm{P}} \arrow[r, "I'"] \arrow[dd, "z_{\mathrm{K}/\mathrm{P}}"] & W(\overline{\mathrm{K}}/\mathrm{P})/V_{\mathrm{P}} \arrow[r, "R'"] \arrow[dd, "z_{\overline{\mathrm{K}}/\mathrm{P}}"] & W(\overline{\Lambda}/\mathrm{K})/V_{\mathrm{K}} \arrow[dd, "z_{\overline{\Lambda}/\mathrm{K}}"] \arrow[dr, "u'"] & \\
 & & & A(\mathrm{K}) \\
\Phi_{(l)}(\mathrm{K}/\mathrm{P}) \arrow[r, "I"] & \Psi_{(l)}(\mathrm{K}/\mathrm{P}) \arrow[r, "R"] & \Phi(\overline{\Lambda}/\mathrm{K}) \arrow[ur, "u"] &
\end{tikzcd}$$

is commutative.[‡]

Proof. Let a be a factor system in the operative class of $\overline{\Lambda}/\mathrm{K}/\mathrm{P}$, corresponding to the set Γ' of representatives which was used to define $b(\gamma)$ in (5·2). Then $\overline{\gamma\delta}^{-1}\overline{\gamma}\overline{\delta} = a(\gamma, \delta)$ and so for all $\phi \in \Phi(\overline{\Lambda}/\mathrm{K})$, $\phi(\overline{\gamma\delta}^{-1}\overline{\gamma}\overline{\delta}) = \phi(a(\gamma, \delta))$, while in particular from (5·1), (5·3)

$$\theta_{\mathrm{A}}(\overline{\gamma\delta}^{-1}\overline{\gamma}\overline{\delta}) = c_{\mathrm{A}}(\gamma, \delta).$$

It follows that

$$\bar{c}_{\mathrm{A}} = u\theta_{\mathrm{A}}. \tag{5·6}$$

Thus $u'(\mathrm{A}V_{\mathrm{K}}) = uz_{\overline{\Lambda}/\mathrm{K}}(\mathrm{A}V_{\mathrm{K}})$ for all $\mathrm{A} \in W(\overline{\Lambda}/\mathrm{K})$. Hence, first, the image group of u' is $A(\mathrm{K})$, and secondly, the relation $u' = uz_{\Lambda/\mathrm{K}}$ holds. The remaining relations

$$z_{\overline{\mathrm{K}}/\mathrm{P}}I' = Iz_{\mathrm{K}/\mathrm{P}}, \quad z_{\overline{\Lambda}/\mathrm{K}}R' = Rz_{\mathrm{K}/\mathrm{P}}$$

in (ii) follow easily from the definition of the mappings involved. That the sequence S' is exact follows now from (ii) and from theorem 1.

It remains to be shown that $A(\mathrm{K})$ is the kernel in $\overline{F}(\Gamma, E)$ of the mapping y. Let $\bar{c} \in A(\mathrm{K})$; then by what was just proved $\bar{c}$ has a representative c_{A} of form (5·5). But this implies that the class of c_{A} in $\overline{F}(\Gamma, V_{\mathrm{K}})$ is the unit class, and so $y\bar{c} = 1$. Conversely, assume that $y\bar{c} = 1$. Then for any representative c of $\bar{c}$ in $F(\Gamma, E)$, there exists a mapping $b\colon \Gamma \rightarrow V_{\mathrm{K}}$ such that

$$c(\gamma, \delta) = b(\gamma)\,.\,\gamma b(\delta)\,.\,(b(\gamma, \delta))^{-1}, \quad \text{for all } \gamma, \delta \in \Gamma. \tag{5·7}$$

Also

$$c(\gamma, \delta) \in E,$$

i.e.

$$(c(\gamma, \delta))^{l} = 1, \quad \text{for all } \gamma, \delta \in \Gamma. \tag{5·8}$$

Put

$$(b(\gamma))^{l} = \bar{b}(\gamma).$$

[†] $\Phi_{(l)}(\mathrm{K}/\mathrm{P})$, $\Psi_{(l)}(\mathrm{K}/\mathrm{P})$ are the subgroups of $\Phi(\mathrm{K}/\mathrm{P})$, and of $\Psi(\mathrm{K}/\mathrm{P})$ of elements ϕ with $\phi^{l} = 1$. The restriction of I, R to these subgroups is again denoted by the same symbols.

[‡] A diagram of mappings is commutative, if any resultant homomorphism solely depends on the 'end points', but not on the 'path' chosen.

By (5·7), (5·8)

$$\bar{b}(\gamma)\,.\,\gamma\bar{b}(\delta)\,.\,(\bar{b}(\gamma,\delta))^{-1}=1, \quad \text{for all } \gamma,\delta\in\bar{\Gamma}. \tag{5·9}$$

By E. Noether's theorem (cf. Chevalley 1954, p. 8), (5·9) implies the existence of an element α in V_{K} with

$$\gamma\alpha\,.\,\alpha^{-1}=\bar{b}(\gamma), \quad \text{for all } \gamma\in\bar{\Gamma}. \tag{5·10}$$

Put $\mathrm{A}^l=\alpha$. Then $(\mathrm{K}(\mathrm{A}):\mathrm{K})\mid l$; also by (5·10) $\gamma\alpha\,.\,\alpha^{-1}\in V_{\mathrm{K}}^l$, and so $\mathrm{K}(\mathrm{A})$ is a central extension of K over P. Thus $\mathrm{K}(\mathrm{A})\in\mathfrak{C}(\mathrm{K}/\mathrm{P})$, and hence $\mathrm{A}\in W(\bar{\Lambda}/\mathrm{K})$. It is now easily seen that $\overline{c_{\mathrm{A}}c^{-1}}$ is the unit class in $\bar{F}(\Gamma,E)$, i.e. that $\bar{c}=\bar{c}_{\mathrm{A}}\in A(\mathrm{K})$.

6. The associated local sequences

The notation is the same as in § 3. P will from now on be taken as a finite algebraic number field. Let $\mathfrak{p}$ be a prime divisor in P, and let $\mathrm{P}_{\mathfrak{p}}$ be the $\mathfrak{p}$-adic completion of P. $\mathrm{K}_{\mathfrak{p}}$ is the composite field extension $\mathrm{KP}_{\mathfrak{p}}$ of $\mathrm{P}_{\mathfrak{p}}$. On the other hand, $\bar{\Lambda}_{\mathfrak{p}}$ is defined directly as in § 2, as the union of fields in $\mathfrak{C}(\mathrm{K}_{\mathfrak{p}}/\mathrm{P}_{\mathfrak{p}})$; a similar notation, using the subscript $\mathfrak{p}$, is employed as regards the groups and homomorphisms associated with $\mathfrak{C}(\mathrm{K}_{\mathfrak{p}}/\mathrm{P}_{\mathfrak{p}})$. The field $\bar{\Lambda}_{\mathfrak{p}}$ will contain $\bar{\Lambda}\mathrm{P}_{\mathfrak{p}}$ but need not coincide with this field. We note that together with the sequence $S_{\mathrm{K}/\mathrm{P}}=S$ of theorem 1, the sequence $S_{\mathrm{K}\mathfrak{p}/\mathrm{P}\mathfrak{p}}=S_{\mathfrak{p}}$ also will be exact.

P is considered as a joint subfield of $\bar{\Lambda}$ and $\bar{\Lambda}_{\mathfrak{p}}$. There then exists an isomorphism† t of $\bar{\Lambda}$ into $\bar{\Lambda}_{\mathfrak{p}}$ leaving P element-wise fixed; if t' is another such isomorphism, then $t^{-1}t'\in\bar{\Gamma}$. The mapping T defined by $T(\gamma)=t^{-1}\gamma t$ for all $\gamma\in\bar{\Gamma}_{\mathfrak{p}}$ is a homomorphism of $\bar{\Gamma}_{\mathfrak{p}}$ into $\bar{\Gamma}$, unique to within inner automorphisms of $\bar{\Gamma}$. Write T^* for the restriction of T to $\Gamma(\bar{\Lambda}_{\mathfrak{p}}/\mathrm{K}_{\mathfrak{p}})$, and for $\mathrm{M}=\mathrm{K},\bar{\mathrm{K}}$ define the mapping T_{M} of $\Gamma(\mathrm{M}_{\mathfrak{p}}/\mathrm{P}_{\mathfrak{p}})$ into $\Gamma(\mathrm{M}/\mathrm{P})$ by $T_{\mathrm{M}}(\gamma\Gamma(\bar{\Lambda}_{\mathfrak{p}}/\mathrm{M}_{\mathfrak{p}}))=T(\gamma)\,\Gamma_{\mathrm{M}}$. These mappings are properly defined, as $t\mathrm{K}\subseteq\mathrm{K}_{\mathfrak{p}}$, $t\bar{\mathrm{K}}\subseteq\bar{\mathrm{K}}_{\mathfrak{p}}$ and so

$$T\Gamma(\bar{\Lambda}_{\mathfrak{p}}/\mathrm{K}_{\mathfrak{p}})\subseteq\Gamma_{\mathrm{K}}, \quad T\Gamma(\bar{\Lambda}_{\mathfrak{p}}/\bar{\mathrm{K}}_{\mathfrak{p}})\subseteq\Gamma_{\bar{\mathrm{K}}}.$$

We note for future reference that the completion of $t\mathrm{K}$ is $\mathrm{K}_{\mathfrak{p}}$, whence the kernel of T lies in $\Gamma(\bar{\Lambda}_{\mathfrak{p}}/\mathrm{K}_{\mathfrak{p}})$. T_{K} is thus an isomorphism into $\Gamma(\mathrm{K}/\mathrm{P})$ and the inverse image under T of Γ_{K} lies in $\Gamma(\bar{\Lambda}_{\mathfrak{p}}/\mathrm{K}_{\mathfrak{p}})$. Equivalently we could have defined T_{M} directly in terms of the restriction t_{M} of t to M. We note that T^* and T_{M} are uniquely determined‡ by $\mathfrak{p}$.

The formula $\phi_{\mathfrak{p}}(\gamma)=\phi(T_{\mathrm{M}}(\gamma))$, for all $\gamma\in\Gamma(\mathrm{M}_{\mathfrak{p}}/\mathrm{P}_{\mathfrak{p}})$, defines corresponding to each character ϕ of $\Phi(\mathrm{M}/\mathrm{P})$ a character $\phi_{\mathfrak{p}}$ of $\Phi(\mathrm{M}_{\mathfrak{p}}/\mathrm{P}_{\mathfrak{p}})$; here M is one of the symbols $\mathrm{K},\bar{\mathrm{K}}$. The mapping $\phi\to\phi_{\mathfrak{p}}$ is a homomorphism, and as T_{M} was uniquely determined by $\mathfrak{p}$, so is this homomorphism. We note that if ϕ and $\phi_{\mathfrak{p}}$ are interpreted as class-group characters, then $\phi_{\mathfrak{p}}$ is precisely the $\mathfrak{p}$-component of ϕ in the sense of class-field theory.

If $\phi\in\Phi(\bar{\Lambda}/\mathrm{K})$, then the equation $\phi_{\mathfrak{p}}(\gamma)=\phi(T^*(\gamma))$ for all $\gamma\in\Gamma(\bar{\Lambda}_{\mathfrak{p}}/\mathrm{K}_{\mathfrak{p}})$ defines a character $\phi_{\mathfrak{p}}$ in $\Phi(\bar{\Lambda}_{\mathfrak{p}}/\mathrm{K}_{\mathfrak{p}})$. The mapping $\phi\to\phi_{\mathfrak{p}}$ of $\Phi(\bar{\Lambda}/\mathrm{K})$ into $\Phi(\bar{\Lambda}_{\mathfrak{p}}/\mathrm{K}_{\mathfrak{p}})$ is a homomorphism, uniquely determined by $\mathfrak{p}$. To obtain a class-field interpretation of this mapping we observe that the restriction t_{K} of t to K can be extended to a value isomorphism $t_{\mathfrak{P}}$ of the $\mathfrak{P}$-adic completion $\mathrm{K}_{\mathfrak{P}}$ of K onto $\mathrm{K}_{\mathfrak{p}}$, the prime divisor $\mathfrak{P}$ lying above $\mathfrak{p}$, and we can obtain such an isomorphism $t_{\mathfrak{P}}$ for each prime divisor $\mathfrak{P}$ in K, lying above $\mathfrak{p}$, by a suitable choice of t. We then have for all $\phi\in\Phi(\bar{\Lambda}/\mathrm{K})$, and for all idèles $\mathfrak{a}$ in K, $\phi(\mathfrak{a}_{\mathfrak{P}})=\phi_{\mathfrak{p}}(t_{\mathfrak{P}}(\mathfrak{a}_{\mathfrak{P}}))$.

† t operates on the left.

‡ A mapping is said to be uniquely determined by $\mathfrak{p}$, if it solely depends on $\mathfrak{p}$, and of course on K, but not on the choice of t.

Finally, let $c \in F(\Gamma, E)$. Then the equations

$$c_{\mathfrak{p}}(\gamma, \delta) = c(T_{\mathrm{K}}(\gamma), T_{\mathrm{K}}(\delta)), \quad \text{all } \gamma, \delta \in \Gamma_{\mathfrak{p}}$$

define an element $c_{\mathfrak{p}} \in F(\Gamma_{\mathfrak{p}}, E)$. Furthermore, $\bar{c}_{\mathfrak{p}}$ depends solely on $\bar{c}$, and $\bar{c} \to \bar{c}_{\mathfrak{p}}$ is a homomorphism of $\overline{F}(\Gamma, E)$ into $\overline{F}(\Gamma_{\mathfrak{p}}, E)$ uniquely determined by $\mathfrak{p}$. One can again interpret this mapping in terms of the idèle group J of P. In fact if c, $c_{\mathfrak{p}}$ are considered as factor systems of J, and of the multiplicative group of $\mathrm{P}_{\mathfrak{p}}$, as in the concluding remarks of § 3, then† for all $\mathfrak{a}, \mathfrak{b} \in J$

$$c_{\mathfrak{p}}(\mathfrak{a}_{\mathfrak{p}}, \mathfrak{b}_{\mathfrak{p}}) = c(\mathfrak{a}_{\mathfrak{p}}, \mathfrak{b}_{\mathfrak{p}}).$$

One can also define $c_{\mathfrak{p}}$ directly as a factor system of J by

$$c_{\mathfrak{p}}(\mathfrak{a}, \mathfrak{b}) = c(\mathfrak{a}_{\mathfrak{p}}, \mathfrak{b}_{\mathfrak{p}}).$$

For the purpose of stating the following theorem, denote by $s_{\mathfrak{p}}$ the mapping of

$$\overline{F}(\Gamma, E) \to \overline{F}(\Gamma_{\mathfrak{p}}, E)$$

given by the rule $\bar{c} \to \bar{c}_{\mathfrak{p}}$, and by $v_{\mathfrak{p}}$, $\bar{v}_{\mathfrak{p}}$, $v_{\mathfrak{p}}^*$, respectively, the three mappings

$$\Phi(\mathrm{K}/\mathrm{P}) \to \Phi(\mathrm{K}_{\mathfrak{p}}/\mathrm{P}_{\mathfrak{p}}), \quad \Psi(\mathrm{K}/\mathrm{P}) \to \Psi(\mathrm{K}_{\mathfrak{p}}/\mathrm{P}_{\mathfrak{p}}), \quad \Phi(\overline{\Lambda}/\mathrm{K}) \to \Phi(\overline{\Lambda}_{\mathfrak{p}}/\mathrm{K}_{\mathfrak{p}})$$

given by the rule $\phi \to \phi_{\mathfrak{p}}$. Then we have

Theorem 4. *The diagram*

$$\begin{tikzcd}
\Phi(\mathrm{K}/\mathrm{P}) \arrow[r, "I"] \arrow[d, "v_{\mathfrak{p}}"] & \Psi(\mathrm{K}/\mathrm{P}) \arrow[r, "R"] \arrow[d, "\bar{v}_{\mathfrak{p}}"] & \Phi(\overline{\Lambda}/\mathrm{K}) \arrow[r, "u"] \arrow[d, "v_{\mathfrak{p}}^*"] & A(\mathrm{K}) \arrow[d, "s_{\mathfrak{p}}"] \\
\Phi(\mathrm{K}_{\mathfrak{p}}/\mathrm{P}_{\mathfrak{p}}) \arrow[r, "I_{\mathfrak{p}}"] & \Psi(\mathrm{K}_{\mathfrak{p}}/\mathrm{P}_{\mathfrak{p}}) \arrow[r, "R_{\mathfrak{p}}"] & \Phi(\overline{\Lambda}_{\mathfrak{p}}/\mathrm{K}_{\mathfrak{p}}) \arrow[r, "u_{\mathfrak{p}}"] & A(\mathrm{K}_{\mathfrak{p}})
\end{tikzcd}$$

is commutative.‡

Proof. The first commutativity relation $\bar{v}_{\mathfrak{p}} I = I_{\mathfrak{p}} v_{\mathfrak{p}}$ is trivial. Next let

$$\psi \in \Psi(\mathrm{K}/\mathrm{P}), \quad \gamma \in \Gamma(\overline{\Lambda}_{\mathfrak{p}}/\mathrm{K}_{\mathfrak{p}}).$$

Then

$$\begin{aligned}[v_{\mathfrak{p}}^* R\psi](\gamma) &= [R\psi](T^*(\gamma)) = \psi(T^*(\gamma)\,\Gamma_{\overline{\mathrm{K}}}) = \psi(T(\gamma)\,\Gamma_{\overline{\mathrm{K}}}) = \psi(T_{\mathrm{K}}(\gamma\Gamma(\overline{\Lambda}_{\mathfrak{p}}/\overline{\mathrm{K}}_{\mathfrak{p}}))) \\ &= [\bar{v}_{\mathfrak{p}}\psi](\gamma\Gamma(\overline{\Lambda}_{\mathfrak{p}}/\overline{\mathrm{K}}_{\mathfrak{p}})) = [R_{\mathfrak{p}}\bar{v}_{\mathfrak{p}}\psi](\gamma).\end{aligned}$$

It follows that

$$v_{\mathfrak{p}}^* R = R_{\mathfrak{p}} \bar{v}_{\mathfrak{p}}.$$

Let now $a_{\mathfrak{p}}$ be a representative of $\bar{a}(\mathrm{K}_{\mathfrak{p}})$ in $F(\Gamma_{\mathfrak{p}}, \Gamma(\overline{\Lambda}_{\mathfrak{p}}/\mathrm{K}_{\mathfrak{p}}))$. One can assume that $a_{\mathfrak{p}}$ corresponds to the complete set $\Gamma_{\mathfrak{p}}'$ of representatives of $\Gamma_{\mathfrak{p}}$ in $\overline{\Gamma}_{\mathfrak{p}}$ (cf. § 2). As the mapping T_{K} is biunique the images under T of distinct elements in $\Gamma_{\mathfrak{p}}'$ lie in distinct cosets of $\overline{\Gamma}$ mod Γ_{K}. Hence, T maps $\Gamma_{\mathfrak{p}}'$ biuniquely into a complete set Γ' of representatives of Γ in $\overline{\Gamma}$. Let a be the factor system in $F(\Gamma, \Gamma_{\mathrm{K}})$ corresponding to Γ'. Then, first, $\bar{a} = \bar{a}(\mathrm{K})$, and in the second place

$$T(a_{\mathfrak{p}}(\gamma, \delta)) = a(T_{\mathrm{K}}(\gamma), T_{\mathrm{K}}(\delta)),$$

whence also

$$T^*(a_{\mathfrak{p}}(\gamma, \delta)) = a(T_{\mathrm{K}}(\gamma), T_{\mathrm{K}}(\delta)), \quad \text{for all } \gamma, \delta \in \Gamma_{\mathfrak{p}}. \tag{6·1}$$

Put for $\phi \in \Phi(\overline{\Lambda}/\mathrm{K})$, and for all $\gamma_1, \gamma_2 \in \Gamma$, $c(\gamma_1, \gamma_2) = \phi(a(\gamma_1, \gamma_2))$. Then $\bar{c} = u\phi$.

† Here as already earlier on we identify the $\mathfrak{p}$ component $\mathfrak{a}_{\mathfrak{p}}$ of an idèle $\mathfrak{a}$ with the corresponding element in $\mathrm{P}_{\mathfrak{p}}$.

‡ The meaning of the symbols $I_{\mathfrak{p}}$, $R_{\mathfrak{p}}$, $u_{\mathfrak{p}}$ is the obvious one.

Write $$c_{\mathfrak{p}}(\gamma, \delta) = c(T_{\mathrm{K}}(\gamma), T_{\mathrm{K}}(\delta)), \quad \text{for all } \gamma, \delta \in \Gamma_{\mathfrak{p}}. \tag{6·2}$$

Then $\bar{c}_{\mathfrak{p}} = s_{\mathfrak{p}} u\phi$. But by (6·1)
$$c_{\mathfrak{p}}(\gamma, \delta) = \phi(T^*(a_{\mathfrak{p}}(\gamma, \delta))),$$
which implies $\bar{c}_{\mathfrak{p}} = u_{\mathfrak{p}} v^*_{\mathfrak{p}} \phi$. Theorem 4 is thus established.

Let X(P) be the group† of residue characters modulo finite divisors in P. If $\phi \in \Phi(\mathrm{P})$, and if G is the set of finite prime divisors in P ramified at ϕ, denote by $w\phi$ the restriction of $\prod_G \phi_{\mathfrak{p}}$ to the group of numbers which are units at all prime divisors of G. w is then a homomorphism of $\Phi(\mathrm{P})$ into X(P). Next, if $\phi_{\mathfrak{p}} \in \Phi(\mathrm{P}_{\mathfrak{p}})$, denote the restriction of $\phi_{\mathfrak{p}}$ to the units at $\mathfrak{p}$ by $w_{\mathfrak{p}}\phi_{\mathfrak{p}}$. If $\phi_{\mathfrak{p}}$ is considered as a character of a Galois group, $w_{\mathfrak{p}}\phi_{\mathfrak{p}}$ is its restriction to the inertia group. The operators w and $w_{\mathfrak{p}}$ are then connected by the equation $w\phi = \prod_G w_{\mathfrak{p}}\phi_{\mathfrak{p}}$ for all $\phi \in \Phi(\mathrm{P})$.

In a similar manner define for any prime divisor $\mathfrak{p}$ in P and for all $\phi_{\mathfrak{p}} \in \Phi(\bar{\Lambda}_{\mathfrak{p}}/\mathrm{K}_{\mathfrak{p}})$ characters $\bar{w}_{\mathfrak{p}}\phi_{\mathfrak{p}}$, either as the restriction of $\phi_{\mathfrak{p}}$ to the units of $\mathrm{K}_{\mathfrak{p}}$, or as the restriction to the inertia group $\mathrm{T}(\bar{\Lambda}_{\mathfrak{p}}/\mathrm{K}_{\mathfrak{p}})$ in $\Gamma(\bar{\Lambda}_{\mathfrak{p}}/\mathrm{K}_{\mathfrak{p}})$. Define the character $r_{\mathfrak{p}} w_{\mathfrak{p}} \psi_{\mathfrak{p}}$, for $\psi_{\mathfrak{p}} \in \Psi(\mathrm{K}_{\mathfrak{p}}/\mathrm{P}_{\mathfrak{p}})$ by
$$[r_{\mathfrak{p}} w_{\mathfrak{p}} \psi_{\mathfrak{p}}]\,(\gamma) = [w_{\mathfrak{p}}\psi_{\mathfrak{p}}]\,(\gamma\Gamma(\bar{\Lambda}_{\mathfrak{p}}/\bar{\mathrm{K}}_{\mathfrak{p}}),$$
for all $\gamma \in \mathrm{T}(\bar{\Lambda}_{\mathfrak{p}}/\mathrm{K}_{\mathfrak{p}})$. Then $r_{\mathfrak{p}}$ is a homomorphism of $w_{\mathfrak{p}}\Psi(\mathrm{K}_{\mathfrak{p}}/\mathrm{P}_{\mathfrak{p}})$ into $\bar{w}_{\mathfrak{p}}\Phi(\bar{\Lambda}_{\mathfrak{p}}/\mathrm{K}_{\mathfrak{p}})$, and
$$\bar{w}_{\mathfrak{p}} R_{\mathfrak{p}} = r_{\mathfrak{p}} w_{\mathfrak{p}}. \tag{6·3}$$

Once the results of this section have been established the notation to be used in the remainder of this paper can be simplified. Thus, no use will be made of the symbols $v_{\mathfrak{p}}$, $s_{\mathfrak{p}}$, etc., occurring in theorem 4 and instead the $\mathfrak{p}$-component of a character or factor-system class f will simply be denoted by $f_{\mathfrak{p}}$. Also, throughout, the symbol $w_{\mathfrak{p}}\phi$ will be used for the restrictions of ϕ to the units at $\mathfrak{p}$, or at the prime divisors lying above $\mathfrak{p}$, whether $\phi \in \Phi(\mathrm{M})$, or $\phi \in \Phi(\mathrm{M}_{\mathfrak{p}})$, for M = P or M = K. No confusion can arise as in each case it will be clear on which characters the operator $w_{\mathfrak{p}}$ is defined.

7. The exact sequence with rational base field

The preceding sections have prepared the formal apparatus which will now be applied to the case when P is the rational field. Our aim is a determination of $\mathfrak{C}(\mathrm{K}/\mathrm{P})$ in terms of the rational field. More precisely, having shown in §§ 3, 6, how the structure of $\mathfrak{C}(\mathrm{K}/\mathrm{P})$ is described in terms of formal invariants, we shall want to derive a rational determination of these invariants. By a determination of groups which appear as such description invariants one has to understand of course not just their determination as abstract groups, but an algebraic or arithmetic characterization as concrete groups, i.e. groups of characters or factor-system classes, which among other things would enable one in each case to find the abstract group structure. Thus theorems 6 and 7 determine $A(\mathrm{K})$ not as an abstract group but as a subgroup of $\bar{F}(\Gamma, E)$ given by certain relations. For the group $\Phi(\bar{\Lambda}/\mathrm{K})$ the structure problem is in any case trivial; this group is the direct product of $\aleph_0$ groups of order l; what one should have in mind is rather an explicit representation of the elements ϕ of $\Phi(\bar{\Lambda}/\mathrm{K})$, which—to give an example—will make it possible to determine for each ϕ the element $u\phi$ and thus the operative type for $\mathrm{K}_{\phi}/\mathrm{K}/\mathrm{P}$.

† With the appropriate convention of equality the residue characters form a group.

The field K is given only as a class field of P, e.g. in terms of $\Phi(\mathrm{K}/\mathrm{P})$. We cannot assume any further information on K. With $\Phi(\mathrm{K}/\mathrm{P})$, however, the group $\Psi(\mathrm{K}/\mathrm{P})$ and the injection mapping I are known as well. Here again, we 'know' these groups not merely as abstract groups, but as groups of idèle class characters with given algebraic and arithmetical properties. Similarly, the operator R, and its image group, can be taken as known; for if $\phi = R\psi$, then K_ϕ is a class field of P with character group $[\Phi(\mathrm{K}/\mathrm{P}), \psi]$. Finally, the group Γ is explicitly given, e.g. by the Artin reciprocity mapping, and hence $\overline{F}(\Gamma, E)$ is given. Similar remarks apply to the corresponding local invariants.

Theorem 1 implies the existence of a group Φ^* such that† $\Phi(\overline{\Lambda}/\mathrm{K}) = \Phi^* \times R\Psi(\mathrm{K}/\mathrm{P})$, $\Phi^* \cong A(\mathrm{K})$. This purely formal observation is, however, useless here; there is, except in special cases, no unique canonical procedure to define such a group Φ^* for any given field K. Instead we shall associate with each field K an arithmetically significant finite subgroup $\Phi^*(\overline{\Lambda}/\mathrm{K})$ of $\Phi(\overline{\Lambda}/\mathrm{K})$ which, however, does not quite possess the simple formal properties postulated above.

Denote by G the set of finite prime divisors in P which are ramified in K, and by F the set of finite prime divisors in P which are non-ramifield in K. Let $\Phi^*(\mathrm{P})$, $\Phi^*(\mathrm{K}/\mathrm{P})$, and $\Psi^*(\mathrm{K}/\mathrm{P})$ be the subgroups of $\Phi(\mathrm{P})$, $\Phi(\mathrm{K}/\mathrm{P})$ and $\Psi(\mathrm{K}/\mathrm{P})$, respectively, of characters ϕ which are non-ramified at the prime divisors in F, and let $\Phi_*(\mathrm{P})$, $\Phi_*(\mathrm{K}/\mathrm{P})$, $\Psi_*(\mathrm{K}/\mathrm{P})$ be the corresponding subgroups of characters ϕ which are not ramified at the prime divisors in G. Then we have

$$\Phi(\mathrm{P}) = \Phi_*(\mathrm{P}) \times \Phi^*(\mathrm{P}), \tag{7·1}$$

$$\Phi_*(\mathrm{K}/\mathrm{P}) = 1, \quad \Phi^*(\mathrm{K}/\mathrm{P}) = \Phi(\mathrm{K}/\mathrm{P}). \tag{7·2}$$

The decomposition (7·1) remains true if we replace all groups by the corresponding maximal subgroups of exponent l. By (7·2) we then get also

$$\Psi(\mathrm{K}/\mathrm{P}) = \Psi_*(\mathrm{K}/\mathrm{P}) \times \Psi^*(\mathrm{K}/\mathrm{P}). \tag{7·3}$$

Denote by $\overline{G}$ and $\overline{F}$ the sets of prime divisors in K lying above those in G, and F, respectively. For $\Phi(\overline{\Lambda}/\mathrm{K})$ a decomposition by precisely the same method as that used above will in general not be possible. In fact, if we were to define $\Phi_*(\mathrm{K})$, $\Phi^*(\mathrm{K})$ in analogy to $\Phi_*(\mathrm{P})$, $\Phi^*(\mathrm{P})$, neither of the relation $\Phi_*(\mathrm{K})\Phi^*(\mathrm{K}) = \Phi(\mathrm{K})$, $\Phi^*(\mathrm{K}) \cap \Phi_*(\mathrm{K}) = 1$ need hold. We define in fact $\Phi^*(\overline{\Lambda}/\mathrm{K})$ as the subgroup of characters in $\Phi(\overline{\Lambda}/\mathrm{K})$ which are non-ramified at all prime divisors in $\overline{F}$. The second component of our decomposition is then given by the group $\Phi_*(\overline{\Lambda}/\mathrm{K}) = R\Psi_*(\mathrm{K}/\mathrm{P})$.

Next write $u\Phi_*(\overline{\Lambda}/\mathrm{K}) = A_*(\mathrm{K})$, $u\Phi^*(\overline{\Lambda}/\mathrm{K}) = A^*(\mathrm{K})$. We denote the restrictions of a mapping $g\colon B \to C$, to the direct components B_*, and B^* by g_* and g^*, respectively, and define $g_* \times g^*$ by $g_* \times g^*(b_* . b^*) = g_*(b_*) . g^*(b^*)$.

THEOREM 5

(i) $\begin{cases} \Phi(\mathrm{K}/\mathrm{P}) = \Phi_*(\mathrm{K}/\mathrm{P}) \times \Phi^*(\mathrm{K}/\mathrm{P}), & \Psi(\mathrm{K}/\mathrm{P}) = \Psi_*(\mathrm{K}/\mathrm{P}) \times \Psi^*(\mathrm{K}/\mathrm{P}), \\ \Phi(\overline{\Lambda}/\mathrm{K}) = \Phi_*(\overline{\Lambda}/\mathrm{K}) \times \Phi^*(\overline{\Lambda}/\mathrm{K}), & A(\mathrm{K}) = A_*(\mathrm{K}) \times A^*(\mathrm{K}). \end{cases}$

(ii) $\Phi^*(\mathrm{K}/\mathrm{P}) = \Phi(\mathrm{K}/\mathrm{P})$, $A^*(\mathrm{K}) = A(\mathrm{K})$, $\Phi_*(\mathrm{K}/\mathrm{P}) = 1$, $A_*(\mathrm{K}) = 1$.

(iii) $I = I_* \times I^*$, $R = R_* \times R^*$, $u = u_* \times u^*$.

† $A \times B$ stands for the direct product of groups A and B.

(iv) *The sequences of homomorphisms*

$$S_*:\quad 1\rightarrow\Phi_*(\mathrm{K/P})\xrightarrow{I_*}\Psi_*(\mathrm{K/P})\xrightarrow{R_*}\Phi_*(\bar\Lambda/\mathrm{K})\xrightarrow{u_*}A_*(\mathrm{K})\rightarrow 1,$$
$$S^*:\quad 1\rightarrow\Phi^*(\mathrm{K/P})\xrightarrow{I^*}\Psi^*(\mathrm{K/P})\xrightarrow{R^*}\Phi^*(\bar\Lambda/\mathrm{K})\xrightarrow{u^*}A^*(\mathrm{K})\rightarrow 1$$

are exact.

From the theorem one gets immediately the following important corollaries:

Corollary 1. *If there exists a field* $\Lambda\in\mathfrak{C}(\mathrm{K/P})$ *with given operative factor-system type, then there also exists such a field whose discriminant is divisible only by the discriminant prime divisors of* K *and by no other primes.*

Corollary 2. *The sequence of homomorphisms*

$$1\rightarrow\Psi_*(\mathrm{K/P})\xrightarrow{R_*}\Phi_*(\bar\Lambda/\mathrm{K})\rightarrow 1$$

is exact. The sequence of homomorphisms

$$1\rightarrow\Phi^*(\bar\Lambda/\mathrm{K})\xrightarrow{u^*}A(\mathrm{K})\rightarrow 1$$

is exact, if and only if $\Phi(\mathrm{K/P})=\Psi^*(\mathrm{K/P})$.

Proof of theorem 5. It will be shown that

$$\Phi_*(\bar\Lambda/\mathrm{K})\cap\Phi^*(\bar\Lambda/\mathrm{K})=1, \tag{7·4}$$
$$\Phi_*(\bar\Lambda/\mathrm{K})\,\Phi^*(\bar\Lambda/\mathrm{K})=\Phi(\bar\Lambda/\mathrm{K}). \tag{7·5}$$

Once (7·4), (7·5) are established, we see by theorem 1 that $u\Phi_*(\bar\Lambda/\mathrm{K})=A_*(\mathrm{K})=1$. (i), (ii), (iii) follow then by using also (7·1) to (7·3). Finally, it is easily verified that the mappings f_* and f^* can be considered as homomorphisms into 'lower star', and 'upper star' groups respectively. (iv) then follows by (i) to (iii) and theorem 1.

To prove (7·4) it will be shown first that if $\mathfrak{p}\in F$, then

$$w_\mathfrak{p}\Psi(\mathrm{K}_\mathfrak{p}/\mathrm{P}_\mathfrak{p})\cong\bar w_\mathfrak{p}R_\mathfrak{p}\Psi(\mathrm{K}_\mathfrak{p}/\mathrm{P}_\mathfrak{p}), \tag{7·6}$$

the isomorphism being induced by the mapping $r_\mathfrak{p}$ defined at the end of §6. In fact the kernel of $r_\mathfrak{p}$ is the group $w_\mathfrak{p}\Phi(\mathrm{K}_\mathfrak{p}/\mathrm{P}_\mathfrak{p})$. But as $\mathfrak{p}$ is non-ramified in K this is the unit group, and so (7·6) follows.

Assume now that $\psi\in\Psi_*(\mathrm{K/P})$, and that $R\psi\in\Phi^*(\bar\Lambda/\mathrm{K})$. We shall see that $\psi=1$; *a fortiori* $R\psi=1$, and so (7·4) holds. By the hypothesis on $R\psi$, this character is not ramified at any prime divisor in $\bar F$. Therefore, by (7·6) ψ is not ramified at any prime divisor in F. But as $\psi\in\Psi_*(\mathrm{K/P})$, ψ is not ramified at any prime divisor in G. Thus ψ is a character in $\Phi(\mathrm{P})$, non-ramified at every finite prime divisor. Therefore $\psi=1$.

The most important and difficult step in the proof of theorem 5 is the proof of (7·5). Here use will be made of the theory of fields of class two (cf. Fröhlich 1954). Let, for any finite rational integral divisor $\mathfrak{m}$, $\mathrm{K}(\mathfrak{m})$ be the maximal Abelian field mod $\mathfrak{m}p_\infty$ whose degree is some power of l, and let whenever $(2^{t+1},\mathfrak{m})=2^t$, with $t=0$, or $t\geqq 4$, $\mathrm{M}(\mathfrak{m})$ be the (unique) maximal field of class two with maximal Abelian subfield $\mathrm{K}(\mathfrak{m})$ as defined by Fröhlich (1954, theorem 4).

Let now $\phi\in\Phi(\bar\Lambda/\mathrm{K})$. Denote by $\bar F_\phi$ the set of all prime divisors in $\bar F$ which are ramified at ϕ; these are the finite prime divisors ramified in $\mathrm{K}_\phi/\mathrm{K}$, but not in K/P. Let F_ϕ be the set of prime divisors in P lying below those in $\bar F_\phi$. Then (Fröhlich 1954, p. 241) K_ϕ will be a subfield of some field $\mathrm{M}(\mathfrak{m})$. If $\mathfrak{m} = \mathfrak{m}'\mathfrak{m}''$, and if all prime divisors contained in $\mathfrak{m}''$ lie outside $G \cup F_\phi$, then K_ϕ will also be a subfield of $\mathrm{M}(\mathfrak{m}')$ (Fröhlich 1954, p. 241). One may thus write $\mathfrak{m} = \mathfrak{m}_1\mathfrak{m}_2$, where $\mathfrak{m}_1$ is a product of divisors in G, and $\mathfrak{m}_2$ is a product of divisors in F_ϕ.

The field K_ϕ is a central extension† of K over P, whence $\mathrm{K}_\phi\mathrm{K}(\mathfrak{m}_1)$ is a central extension of $\mathrm{K}(\mathfrak{m}_1)$ over P, contained in $\mathrm{M}(\mathfrak{m})$. The maximal central extension of $\mathrm{K}(\mathfrak{m}_1)$ over P in $\mathrm{M}(\mathfrak{m})$ is however the field $\mathrm{M}(\mathfrak{m}_1)\,\mathrm{K}(\mathfrak{m})$. Writing $R_{\mathrm{K}/\mathrm{K}(\mathfrak{m}_1)}\,\phi = \bar{\phi}$, we get

$$\bar{\phi} = \bar{\phi}_1\bar{\phi}_2, \quad \phi_1 \in \Phi(\mathrm{M}(\mathfrak{m}_1)/\mathrm{K}(\mathfrak{m}_1)), \quad \bar{\phi}_2 \in \Phi(\mathrm{K}(\mathfrak{m})/\mathrm{K}(\mathfrak{m}_1)).$$

As $\mathrm{K}(\mathfrak{m})$ is the product of the two independent Abelian fields $\mathrm{K}(\mathfrak{m}_1)$ and $\mathrm{K}(\mathfrak{m}_2)$ it follows that $\bar{\phi}_2 = R_{\mathrm{P}/\mathrm{K}(\mathfrak{m}_1)}\psi_2$, $\psi_2 \in \Phi(\mathrm{K}(\mathfrak{m}_2)/\mathrm{P})$. The kernel of $R_{\mathrm{P}/\mathrm{K}(\mathfrak{m}_1)}$ is $\Phi(\mathrm{K}(\mathfrak{m}_1)/\mathrm{P})$. But as $\Phi(\mathrm{K}(\mathfrak{m}_1)/\mathrm{P}) \cap \Phi(\mathrm{K}(\mathfrak{m}_2)/\mathrm{P}) = 1$, it follows that the order of $\bar{\phi}_2$ = order of ψ_2. On the other hand $\mathrm{K}(\mathfrak{m}_1)$ is the maximal Abelian subfield of $\mathrm{M}(\mathfrak{m}_1)$ and so

$$\Phi(\mathrm{K}(\mathfrak{m})/\mathrm{K}(\mathfrak{m}_1)) \cap \Phi(\mathrm{M}(\mathfrak{m}_1)/\mathrm{K}(\mathfrak{m}_1)) = 1.$$

Hence, the order of $\bar{\phi}_2$ is a divisor of the order of $\bar{\phi}$, and hence is a divisor of the order of ϕ. We conclude that $\psi_2^l = 1$. As no prime divisor in G is contained in $\mathfrak{m}_2$ we conclude that $\psi_2 \in \Psi_*(\mathrm{K}/\mathrm{P})$. Write $R_{\mathrm{P}/\mathrm{K}}\psi_2 = \phi_2$, then $\phi_2 \in \Phi_*(\bar{\Lambda}/\mathrm{K})$ and $\phi = \phi_1\phi_2$, where $R_{\mathrm{K}/\mathrm{K}(\mathfrak{m}_1)}\,\phi_1 = \phi_1$. Finally, observe that by the definition of $\bar{\phi}_1$, no prime divisor in $\bar{F}$ is ramified in

$$(\mathrm{K}(\mathfrak{m}_1))_{\bar{\phi}_1} = \mathrm{K}(\mathfrak{m}_1)\,\mathrm{K}_{\phi_1}.$$

The same is then true for the field K_{ϕ_1}, and so $\phi_1 \in \Phi^*(\bar{\Lambda}/\mathrm{K})$. It has thus been proved that every character ϕ in $\Phi(\bar{\Lambda}/\mathrm{K})$ has a decomposition $\phi = \phi_1\phi_2$ in accordance with (7·5).

8. The invariant criterion for $A(\mathrm{K})$

The theorem established in § 7, reduces our problem to that of determining the unknown 'part' $\Phi^*(\bar{\Lambda}/\mathrm{K}) \xrightarrow{u^*} A^*(\mathrm{K})$ of the sequence S^*.

Denote the finite part of the conductor of K by f and write

$$f^* = f \quad \text{if} \quad (f, l) = 1, \tag{8·1 a}$$

$$f^* = fl \quad \text{if} \quad 2 \neq l \quad \text{and} \quad l^2 \mid f, \quad \text{or if} \quad 2 = l \quad \text{and} \quad 8 \mid f, \tag{8·1 b}$$

$$f^* = fl^2 \quad \text{if} \quad 2 = l \quad \text{and} \quad (8, f) = 4. \tag{8·1 c}$$

Put $\Lambda^* = \bar{\Lambda} \cap \mathrm{M}(f^*)$; then it will be shown that

$$\Phi(\Lambda^*/\mathrm{K}) = \Phi^*(\bar{\Lambda}/\mathrm{K}). \tag{8·2}$$

Let Λ' be the subfield of $\bar{\Lambda}$ belonging to $\Phi^*(\bar{\Lambda}/\mathrm{K})$; we have to prove that $\Lambda' = \Lambda^*$. In the first place, $\Lambda^* \subseteq \bar{\Lambda}$. Also, the prime divisors in $\bar{F}$ are non-ramified in $\mathrm{M}(f^*)/\mathrm{K}$, and *a fortiori* in Λ^*/K. Therefore $\Phi(\Lambda^*/\mathrm{K}) \subseteq \Phi^*(\bar{\Lambda}/\mathrm{K})$, i.e. $\Lambda^* \subseteq \Lambda'$.

For the converse, let $\phi \in \Phi^*(\bar{\Lambda}/\mathrm{K})$. Then $\mathrm{K}_\phi \subseteq \mathrm{M}(\mathfrak{m})$ for some $\mathfrak{m}$. By an argument already used in § 7, one may take $\mathfrak{m}$ to be a product of prime divisors in G; and as $\mathrm{K} \subseteq \mathrm{M}(\mathfrak{m})$, we have $f \mid \mathfrak{m}$. Put

$$f = \prod_i p_i^{s_i} \quad (s_i > 0,\ p_i \text{ prime}), \quad \mathfrak{m} = \prod_i p_i^{s_i + r_i}\,(r_i \geqq 0).$$

If now $p_i \neq l$, then $s_i = 1$, and $\mathrm{K}(\mathfrak{m}'p_i^2) = \mathrm{K}(\mathfrak{m}'p_i)$ for all $\mathfrak{m}'$, whence also $\mathrm{M}(\mathfrak{m}'p_i^2) = \mathrm{M}(\mathfrak{m}'p_i)$. One may thus assume

$$f = l^q f_1, \quad \mathfrak{m} = l^{q+r} f_1, \quad (l, f_1) = 1. \tag{8·3}$$

† See footnote §, p. 390.

We shall see that in all cases we may take $\mathfrak{m} = f^*$. This then implies $\Lambda' \subseteq \mathrm{M}(f^*)$, i.e. $\Lambda' \subseteq \Lambda^*$. In fact, if $q = 0$, then by the previous convention $r = 0$, and so $\mathfrak{m} = f^*$. Otherwise we have $q \geqq 2$. Put $f' = f$, if $l \neq 2$, or if $8 \mid f$, and put $f' = fl$, if $l = 2$, $(8, f) = 4$. Then $\mathrm{K}(f') \supseteq \mathrm{K}$, and $\mathrm{K}_\phi \mathrm{K}(f')$ is a central extension of $\mathrm{K}(f')$ over P whose relative degree divides l. But (Fröhlich 1954, theorem 5, 7) this implies $\mathrm{K}_\phi \mathrm{K}(f') \subseteq \mathrm{M}(lf')$; i.e. we may take $\mathfrak{m} = lf = f^*$.

Using (8·2) and the homomorphism u^* one can now derive the group $A(\mathrm{K})$.

Theorem 6. *In order that the class $\bar{c}$ of a factor system c in $F(\Gamma, E)$ lie in $A(\mathrm{K})$ it is necessary and sufficient that*

A. Whenever $p \mid f$, $p \equiv 1 \pmod{l}$, then

(i) $\prod_{r \bmod p-1} c_p(a, a^r) = c_p(a, p)\,(c_p(p, a))^{-1}$ *for all rational idèles a which are units at p. If $2 \mid f$, then*

(ii) $\prod_{r \bmod 2} c_2(-1, (-1)^r) = c_2(5, 2)\,(c_2(2, 5))^{-1}$.

B. If p is of ramification order l^{t_p} in K, *then an equivalent relation to* (i) *is*

(ia) $c_p^*(a)^{p-1/l^{t_p}} = c_{*p}(a, p)$, *and an equivalent relation to* (ii) *is*

(ii$a$) $c_2^*(-1) = c_{*2}(5, 2)$, *where c_p^* is the power factor system, and c_{*p} the commutator factor system associated*† *with $\bar{c}_p$.*

Remarks 1. In (i), (ia), it suffices to take as the range of a the set of all rationals, prime to p. Moreover, if a_p is a primitive root mod p then it is necessary and sufficient to satisfy (i), or (ia) for $a = a_p$ only. In fact if (i) or (ia) holds for all a in the given range, it will hold for $a = a_p$; conversely, if the equations are satisfied for a_p, then they also hold for all powers of a_p; but as $c(a, p)$ solely depends on $a \bmod p$, it follows that (i) and (ia) will hold for all a in the given range.

Proof of theorem 6. Write $\mathrm{K}^* = \mathrm{K}(f^*)$, $\Gamma^* = \Gamma(\mathrm{K}^*/\mathrm{P})$. For each prime p, K_p^* will denote the inertia field of p in K^*. $\mathrm{K}^{*(2)}$ is the unique cyclic field whose conductor is 2^t for which -1 is the total norm residue in P, i.e. $\mathrm{K}^{*(2)}$ is the unique real field of degree 2^{t-2}, whose discriminant is a power of 2. Here $2^t = (f^*, 2^{t+1})$. $\mathrm{K}^{*(2)}$ and $\mathrm{P}(\surd-1)$ are subfields of K^* if $2 \mid f$. Let for $p \equiv 1 \pmod{l}$, a_p be a primitive root mod p. Write for all p

$$\left(\frac{p, \mathrm{K}^*}{p}\right) = \omega_p^*, \tag{8·4}$$

for $p \equiv 1 \pmod{l}$, $p \mid f$

$$\left(\frac{a_p, \mathrm{K}^*}{p}\right) = \sigma_p^*, \tag{8·5a}$$

for $l \mid f$, $l \neq 2$

$$\left(\frac{1+l, \mathrm{K}^*}{l}\right) = \sigma_l^*, \tag{8·5b}$$

for $2 \mid f$

$$\left(\frac{5, \mathrm{K}^*}{2}\right) = \sigma_8^*, \quad \left(\frac{-1, \mathrm{K}^*}{2}\right) = \sigma_4^*. \tag{8·5c}$$

Then for $p \neq 2$, K_p^* is the invariant field of $[\sigma_p^*]$, and for $2 \mid f$, $\mathrm{K}_2^*\,\mathrm{P}(\surd-1)$ is the invariant field of $[\sigma_8^*]$, $\mathrm{K}_2^*\,\mathrm{K}^{*(2)}$ is the invariant field of $[\sigma_4^*]$. The group Γ^* has the basis σ_q^*, the symbol

† As noted in §2, $\bar{c}$ uniquely determines the pair c_*, c^* and vice versa.

q having always as its domain of values the odd primes p dividing f, and if $2 \mid f$ the symbols 4 and 8. A complete set of defining relations† of Γ^* is

$$\Gamma^* \text{ is Abelian, order } \Gamma^* \text{ is a power of } l. \tag{8·6}$$

$$\sigma_p^{*p-1} = 1 \quad \text{if} \quad p \equiv 1 \pmod{l}, \tag{8·7a}$$

$$\sigma_l^{*l^{x}-1} = 1 \quad \text{if} \quad 2 \neq l \mid f, \quad (l^{x+1}, f^*) = l^x, \tag{8·7b}$$

$$\left.\begin{aligned} \sigma_4^{*2} &= 1 \quad (8·7c)\\ \sigma_8^{*2^{x-2}} &= 1 \quad (8·7d)\end{aligned}\right\} \quad \text{if} \quad 2 \mid f, \quad (2^{x+1}, f^*) = 2^x.$$

We now turn to the Galois group $\Omega = \Gamma(\mathrm{M}(f^*)/\Gamma)$ (cf. Fröhlich 1954, theorem 4).‡ K* is the invariant field of the commutator group§ (Ω, Ω). Denote the coset of ω in $\Omega/(\Omega, \Omega) = \Gamma^*$ by ω^*. Let for each symbol q, σ_q be an element of Ω whose coset is σ_q^*, and which lies in a p-inertia group || of Ω, if p is the prime dividing q. Then the elements σ_q generate Ω with defining relations¶

$$(\Omega, (\Omega, \Omega)) = 1, \tag{8·8}$$

$$\text{Order } \Omega \text{ is a power of } l, \tag{8·9}$$

$$\sigma_p^{p-1} = (\sigma_p, \omega_p) \quad \text{if} \quad p \equiv 1 \pmod{l}, \tag{8·10a}$$

$$\sigma_l^{l^{x}-1} = 1 \quad \text{if} \quad 2 \neq l \mid f, \quad (l^{x+1}, f^*) = l^x, \tag{8·10b}$$

$$\left.\begin{aligned} \sigma_4^{2} &= (\sigma_8, \omega_2) \quad (8·10c)\\ \sigma_8^{2^{x-2}} &= 1 \quad (8·10d)\end{aligned}\right\} \quad \text{if} \quad 2 \mid f, \quad (2^{x+1}, f^*) = 2^x.$$

Here ω_p is any representative in Ω of the element ω_p^* of Γ^*, determined by (8·4).

Let now K and Λ^* respectively be the invariant fields of subgroups Δ and Σ of Ω. Δ contains (Ω, Ω), and the group $\Delta^* = \Delta/(\Omega, \Omega)$ is, as a subgroup of Γ^*, given by the character group $\Phi(\mathrm{K}/\mathrm{P})$ of $\Gamma = \Gamma^*/\Delta^*$. Hence, using (8·8) to (8·10), Δ is uniquely determined as a subgroup of Ω by the given character group $\Phi(\mathrm{K}/\mathrm{P})$ only. It will furthermore be shown that

$$\Sigma = \Delta^l(\Delta, \Omega). \tag{8·11}$$

In fact let Λ' be the invariant field of the latter group. As $\Delta/\Delta^l(\Delta, \Omega)$ is Abelian of exponent 1 or l, Λ' is composed of cyclic extensions Λ of K of relative degree 1 or l, and as each such field Λ is fixed under (Δ, Ω), Λ is a central extension of K over P. Therefore $\Lambda \in \mathfrak{C}(\mathrm{K}/\mathrm{P})$, and $\Lambda' \subseteq \Lambda^*$. Conversely, the exponent of $\Gamma(\Lambda^*/\mathrm{K})$ is 1 or l, and so Λ^* is fixed under Δ^l; also Λ^* as a central extension of K over P is fixed under (Δ, Ω). Hence $\Lambda^* \subseteq \Lambda'$, and so finally $\Lambda^* = \Lambda'$.

Denote the coset of an element ω in Ω modulo Δ by ω' and modulo Σ by $\bar{\omega}$. The group $\bar{\Omega} = \Omega/\Sigma$ is then generated by the elements $\bar{\sigma}_q$. The subgroup $\bar{\Delta} = \Delta/\Sigma$ is determined by††

$$\bar{\Delta} \supseteq (\bar{\Omega}, \bar{\Omega}); \quad \text{and} \quad \bar{\omega} \in \bar{\Delta} \quad \text{if and only if} \quad \phi(\omega^*) = 1, \quad \text{for all } \phi \in \Phi(\mathrm{K}/\mathrm{P}). \tag{8·12}$$

† The following relations can be expressed explicitly as relations in the generators. The given form has been chosen for convenience. A similar remark applies at other places in this section.

‡ In applying the results of Fröhlich (1954) certain changes in notation are to be kept in mind. In particular, the elements of Galois groups are now written as left operators and so the order of multiplication has been reversed.

§ In any group Ω the commutator $\omega^{-1}\gamma^{-1}\omega\gamma$ will be denoted by (ω, γ), and if Δ, Σ are non-empty subsets of Ω, the subgroup of Ω generated by the elements (δ, σ), for all $\delta \in \Delta$, all $\sigma \in \Sigma$ will be denoted by (Δ, Σ).

|| A p-inertia group in Ω is the inertia group of some prime divisor $\mathfrak{P}$ in $\mathrm{M}(f^*)$ lying above p.

¶ A remark similar to that in footnote † applies here.

†† See footnote †.

$\overline{\Omega}$ has the defining relations† (8·12), and

$$\overline{\Delta}^l = 1, \tag{8·13}$$

$$(\overline{\Delta}, \overline{\Omega}) = 1, \tag{8·14}$$

together with relations $(\overline{8\cdot 8})$ to $(\overline{8\cdot 10})$, obtained from (8·8) to (8·10) by replacing ω by $\overline{\omega}$. (8·13), (8·14) follow from (8·11). Now $(\overline{8\cdot 8})$ follows from (8·12), (8·14), $(\overline{8\cdot 9})$ from (8·12), (8·13). If $2 \neq l \mid f^*$, then $f^* = lf$ by (6·1). Hence $\phi(\sigma^{*l^{x-2}}) = 1$, for all $\phi \in \Phi(\mathrm{K/P})$, as $(l^x, f) = l^{x-1}$. Hence $(\overline{8\cdot 10b})$ follows from (8·12), (8·13), and the same can be shown for $(\overline{8\cdot 10d})$. We conclude that $(\overline{8\cdot 10a})$, $(\overline{8\cdot 10c})$ and (8·12) to (8·14) represent a complete set of defining relations of $\overline{\Omega}$.

Let now a be a factor system in the operative class for $\Lambda^*/\mathrm{K/P}$. One may assume that for some basis $\mathfrak{g} = [\gamma'_1, \ldots, \gamma'_m]$ of Γ, a is given in the normal form (2·9). Let $\overline{\Delta}_a$ be the subgroup of $\overline{\Delta}$ generated by the elements $a(\omega', \gamma')$ for all $\omega', \gamma' \in \Gamma = \overline{\Omega}/\overline{\Delta}$. Then $\overline{\Delta}_a$ is generated by the elements $a(\gamma'_i, \gamma'^{-1}_i)$, $a(\gamma'_i, \gamma'_j)$ $(i<j)$, and we have:

(i) Γ acts trivially on $\overline{\Delta}_a$ (by (8·14)),

(ii) $\overline{\Delta}^l_a = 1$ (by (8·13)),

(iii) $\prod\limits_{r \bmod p-1} a(\sigma'_p, \sigma'^r_p) = a(\sigma'_p, \omega'_p)\,(a(\omega'_p, \sigma'_p))^{-1}$ if $p \equiv 1 \pmod l$,

$\prod\limits_{r \bmod 2} a(\sigma'_4, \sigma'^r_4) = a(\sigma'_8, \omega'_2)\,(a(\omega'_2, \sigma'_8))^{-1}$,

where for all p, ω'_p is a representative of ω_p, and so $\omega'_p = (p, \mathrm{K}/p)$. ((iii) follows from (8·10a), (8·10c) using the relations

$$(\overline{\omega}, \overline{\gamma}) = a(\omega', \gamma')\,(a(\gamma', \omega'))^{-1}, \quad \overline{\omega}^s = \prod_{r \bmod s} a(\omega', \omega'^r) \quad \text{if} \quad \omega'^s = 1.)$$

(iv) The elements in $\overline{\Delta}_a$ satisfy (2·9). As indicated, (i) to (iv) follow from the defining relations of $\overline{\Omega}$, and moreover (i) to (iv) together with a set of equations

(v) $\sigma'_q = \prod\limits_i \gamma'^{y_{iq}}_i$

giving the representation of the elements σ'_q of Γ in terms of the given basis $\mathfrak{g}$, provide a complete restatement of the defining relations of $\overline{\Omega}$ as far as they affect $\overline{\Delta}_a$. $\overline{\Delta}_a$ is thus the group generated by the elements $a(\gamma'_i, \gamma'^{-1}_i)$, $a(\gamma'_i, \gamma'_j)$ $(i<j)$, with defining relations (ii) to (iv), the elements occurring in (iii) being expressed in terms of the generators by using (v).

Let now $c \in F_{\mathfrak{g}}(\Gamma, E)$. We consider the group E_c generated by the elements $c(\omega', \gamma')$, i.e. by the elements $c(\gamma'_i, \gamma'^{-1}_i)$, $c(\gamma'_i, \gamma'_j)$ $(i<j)$. Then

(ii′) $E^l_c = 1$.

(iv′) The elements of E_c satisfy (2·9).

Let $\phi \in \Phi^*(\overline{\Lambda}/\mathrm{K})$. The function ϕa, defined by $\phi a(\omega', \gamma') = \phi(a(\omega', \gamma'))$ for all $\omega', \gamma' \in \Gamma$ is an element of $F_{\mathfrak{g}}(\Gamma, E)$. Putting $\phi a = c$, we see that not only (ii′) and (iv′) are satisfied but also

(iii′) $\prod\limits_{r \bmod p-1} c(\sigma'_p, \sigma'^r_p) = c(\sigma'_p, \omega'_p)\,(c(\omega'_p, \sigma'_p))^{-1}$ if $p \equiv 1 \pmod l$,

$\prod\limits_{r \bmod 2} c(\sigma'_4, \sigma'^r_4) = c(\sigma'_8, \omega'_2)\,(c(\omega'_2, \sigma'_8))^{-1}$ if $2 \mid f$.

Assume conversely that $c \in F_{\mathfrak{g}}(\Gamma, E)$, and that (iii′) holds. Then the group E_c satisfies (ii′) to (iv′). But as (ii) to (iv) are defining relations of $\overline{\Delta}_a$, the mapping $a(\gamma', \omega') \to c(\gamma', \omega')$ for all $\gamma', \omega' \in \Gamma$ is a homomorphism of $\overline{\Delta}_a$ onto E_c. As furthermore E_c is a subgroup of E

† See footnote † on p. 407.

and $\bar\Delta_a$ is a direct constituent of the elementary Abelian group $\bar\Delta$, it follows that there exists a homomorphism ϕ of $\bar\Delta$ into E, such that for all $\gamma', \omega' \in \Gamma$, $\phi(a(\gamma',\omega')) = c(\gamma',\omega')$. ϕ is then an element of $\Phi^*(\bar\Lambda/\mathrm{K})$, and $c = \phi a$.

Let now $c_1 \in F(\Gamma, E)$, $\bar c_1 \in A(\mathrm{K})$. By theorem 5 $\bar c_1 = u\phi$, $\phi \in \Phi^*(\bar\Lambda/\mathrm{K})$. Let $\bar c_1 = \bar c$, $c \in F_{\mathfrak{g}}(\Gamma, E)$. Then $c = \phi a$, a as above; for, $\overline{\phi a} = \bar c$, $\phi a \in F_{\mathfrak{g}}(\Gamma, E)$, and $F_{\mathfrak{g}}(\Gamma, E)$ contains precisely one representative of $\bar c$. It follows that c satisfies (iii′). But both right- and left-hand sides in (iii′) are expressible in terms of c^*, c_*; in fact we have

$$\prod_{r \bmod n} c(\gamma', \gamma'^r) = c^*(\gamma')^{n/n_{\gamma'}} \tag{8·15}$$

if the order $n_{\gamma'}$ of γ' divides n, and

$$c(\gamma',\omega')\,(c(\omega',\gamma'))^{-1} = c_*(\gamma',\omega'). \tag{8·16}$$

Now c^*, c_* are invariants of the class $\bar c$, and so both sides in (iii′) remain unaltered if c is replaced by c_1. Thus c_1 satisfies (iii′).

Conversely, assume c_1 satisfies (iii′). Then if $\bar c_1 = \bar c$, $c \in F_{\mathfrak{g}}(\Gamma, E)$, c will satisfy (iii′). We saw above that $c = \phi a$, for some $\phi \in \Phi^*(\bar\Lambda/\mathrm{K})$, and so $\bar c = u\phi$, $\bar c_1 \in A(\mathrm{K})$.

It has been shown that $\bar c \in A(\mathrm{K})$, if and only if c satisfies (iii′). It is easily verified that if, for $p \equiv 1 \pmod{l}$,

$$\prod_{r \bmod p-1} c(\sigma'_p, \sigma'^r_p) = c(\sigma'_p, \omega'_p)\,(c(\omega'_p, \sigma'_p))^{-1}$$

then the same equation also holds if σ'_p is throughout replaced by σ'^s_p, for any s. The converse is trivial. Applying Artin's reciprocity mapping we obtain thus theorem 6 (A). Criterion B follows by (8·15), (8·16).

9. Explicit criteria for $A(\mathrm{K})$

The conditions determining $A(\mathrm{K})$ as stated in theorem 6 are invariant in the sense that no explicit reference to any particular characters associated with K or to any particular basis of Γ is involved. For the purpose of computing $A(\mathrm{K})$ in concrete cases it is useful, however, to have an explicit criterion in terms of a given basis of Γ or of $\Phi(\mathrm{K/P})$. Such a criterion will be formulated in theorem 7. At the same time the theorem will throw additional light on the way in which the group $A(\mathrm{K})$ is related to numerical invariants associated with $\Phi(\mathrm{K/P})$. The elements of Γ will now be again denoted by symbols γ, σ, ω instead† of γ', σ', ω'. Otherwise, the notation of § 8 will be adopted. In particular, we shall have to consider again the group $\Gamma(\mathrm{K^*/P})$, whose elements will be denoted as before by σ^*, ω^*, etc. For the complex function $\exp(2\pi i z)$ of a complex variable z we write $\mathrm{e}(z)$.

Let $[l^{n_1}, \ldots, l^{n_m}]$ $(n_i \geqq n_{i+1})$ be the group invariants of $\Phi(\mathrm{K/P})$, i.e. of Γ, and let $[\phi_1, \ldots, \phi_m]$ be a basis of $\Phi(\mathrm{K/P})$, with order $\phi_i = l^{n_i}$. Let $\mathfrak{g} = [\gamma_1, \ldots, \gamma_m]$ be the unique ordered set of elements of Γ satisfying

$$\phi_i(\gamma_j) = \mathrm{e}\,(\delta_{ij}/l^{n_i}) \quad (i, j = 1, \ldots, m). \tag{9·1}$$

Then $\mathfrak{g}$ is a basis of Γ, and order $\gamma_i = l^{n_i}$. Conversely, for such a basis $\mathfrak{g}$, a basis $[\phi_1, \ldots, \phi_m]$ of $\Phi(\mathrm{K/P})$ is defined by (9·1). We put

$$\psi_i = \phi_i^{l^{n_i-1}}. \tag{9·2}$$

Then $[\psi_1, \ldots, \psi_m]$ is a basis‡ of $\Phi_{(l)}(\mathrm{K/P})$.

† No confusion can arise as the group Ω of § 8 will not appear here.

‡ For any Abelian group Φ, $\Phi_{(l)}$ is the subgroup of elements whose lth power is the identity.

Choose for all q† residue characters $\bar{\chi}_q$, χ_q as follows. If $q = p \equiv 1 \pmod{l}$, and if $(p-1, l^{s_q+1}) = l^{s_q}$, $\bar{\chi}_q$ is a residue character mod p of order l^{s_q}. If $2 \neq q = l$ and if

$$(f^*, l^{s_q+2}) = l^{s_q+1},$$

$\bar{\chi}_q$ is a residue character mod l^{s_q+1} of order l^{s_q}. If $q = 8$, $(f^*, 2^{s_q+3}) = 2^{s_q+2}$, χ_q is a residue character mod 2^{s_q+2} of order 2^{s_q}, $\bar{\chi}_q(-1) = 1$. If $q = 4$, $\bar{\chi}_q$ is the residue character mod 4 of order $2^{s_q} = 2$. For all q, $\chi_q = \bar{\chi}_q^{l^{s_q-1}}$; thus χ_q is of order l.

We observe that the mapping w defined in § 6, is now—P being the rational field—an isomorphism of $\Phi(\mathrm{P})$ onto the group $\mathrm{X}(\mathrm{P})$ of rational residue characters. Hence, for all such residue characters χ, $w^{-1}\chi$ is a uniquely defined idèle class character. The characters $w^{-1}\bar{\chi}_q$ then form a basis of $\Phi(\mathrm{K}^*/\mathrm{P})$, and one can assume

$$[w^{-1}\bar{\chi}_{q'}]\,(\sigma_q^*) = \mathrm{e}\,(\delta_{qq'}/l^{s_q}). \tag{9·3}$$

Write for all pairs p, q where $p \mid f$, $(p, q) = 1$,

$$\bar{\chi}_q(p) = \mathrm{e}\,([q,p]/l^{s_q}). \tag{9·4}$$

As $\Phi(\mathrm{K}/\mathrm{P}) \subseteq \Phi(\mathrm{K}^*/\mathrm{P})$ we have a unique representation

$$w\phi_i = \prod_q \bar{\chi}_q^{y_{iq}}, \quad y_{iq} \bmod l^{s_q} \quad (i = 1, \ldots, m). \tag{9·5}$$

The coefficients y_{iq} are given by‡

$$\phi_i(\sigma_q^*) = \mathrm{e}\,(y_{iq}/l^{s_q}), \quad \text{all } i, \text{ all } q. \tag{9·6}$$

As ϕ_i is of order l^{n_i}, there exist integers x_{iq}, such that

$$\mathrm{e}\,(y_{iq}/l^{s_q}) = \mathrm{e}\,(x_{iq}/l^{n_i}) \quad \text{all } i, \text{ all } q. \tag{9·7}$$

For the purpose of formulating theorem 7 it is convenient to introduce in addition to the 'multiplicative' invariants $c^*(\gamma_i)$, $c_*(\gamma_i, \gamma_j)$ also 'additive' invariants $C^*(\gamma_i)$, $C_*(\gamma_i, \gamma_j)$ of the factor-system class $\bar{c}$ in $F(\Gamma, E)$, by

$$c^*(\gamma_i) = \mathrm{e}\,(C^*(\gamma_i)/l), \quad c_*(\gamma_i, \gamma_j) = \mathrm{e}\,(C_*(\gamma_i, \gamma_j)/l), \quad (C^*(\gamma_i),\ C_*(\gamma_i, \gamma_j) \pmod{l}). \tag{9·8}$$

Theorem 7. *A necessary and sufficient condition for the element $\bar{c}$ of $\bar{F}(\Gamma, E)$ to lie in $A(\mathrm{K})$ is that the invariants of $\bar{c}$ satisfy the following conditions.*

A. If $p \equiv 1 \pmod{l}$,§‖ $l \neq 2$,

(i) $\prod_{q(\neq p)} \prod_{i<j} c_*(\gamma_i, \gamma_j)^{[x_{jp}x_{iq} - x_{ip}x_{jq}][q,p]} = \prod_i c^*(\gamma_i)^{x_{ip}(p-1)l^{n_i}}.$

If $p \equiv 1 \pmod{2}$, $l = 2$,

(ii) $\prod_{q(\neq p)} \prod_{i<j} c_*(\gamma_i, \gamma_j)^{[x_{jp}x_{iq} - x_{ip}x_{jq}][q,p]} = \prod_i c^*(\gamma_i)^{x_{ip}(p-1)/2^{n_i}} \prod_{i<j} c_*(\gamma_i, \gamma_j)^{x_{ip}x_{jp}(p-1)/2}.$

If $2 = l$, $2 \mid f$,

(iii) $\prod_{q(\neq 4,8)} \prod_{i<j} c_*(\gamma_i, \gamma_j)^{[x_{j8}x_{iq} - x_{i8}x_{jq}][q,2]} = \prod_i c^*(\gamma_i)^{x_{i4}/2^{n_i-1}} \prod_{i<j} c_*(\gamma_i, \gamma_j)^{x_{i4}x_{j4}}.$

† q has the same range as in § 8.

‡ It should be noted that using the Artin reciprocity mapping all equations of the type (9·6), (9·3), etc., can be expressed as character equations with the elements of the Galois group replaced by idèles.

§ Note that $x_{ip}(p-1)/l^{n_i}$ is integral, by (9·7).

‖ For the symbol $\prod_{i<j}$, see footnote ‡, p. 392.

B. Equivalent to equations (i) *to* (iii) *are*

$$(\mathrm{i}\,a)\ \prod_{p'(\neq p)}\ \prod_{i<j}\{[w_{p'}(\psi_i^{x_{jp}}\psi_j^{-x_{ip}})]\,(p)\}^{C_*(\gamma_i,\gamma_j)}=\prod_i \mathrm{e}\,(x_{ip}(p-1)/l^{n_i+1})^{\,C_*(\gamma_i)}.$$

$$(\mathrm{ii}\,a)\ \prod_{p'(\neq p)}\ \prod_{i<j}\{[w_{p'}(\psi_i^{x_{jp}}\psi_j^{-x_{ip}})]\,(p)\}^{C_*(\gamma_i,\gamma_j)}$$

$$=\prod_i \mathrm{e}\,(x_{ip}(p-1)/2^{n_i+1})^{C^*(\gamma_i)}\prod_{i<j}\mathrm{e}\,(x_{ip}x_{jp}(p-1)/4)^{C_*(\gamma_i,\gamma_j)}.$$

$$(\mathrm{iii}\,a)\ \prod_{p'(\neq p)}\ \prod_{i<j}\{[w_{p'}(\psi_i^{x_{j8}}\psi_j^{-x_{i8}})]\,(2)\}^{C_*(\gamma_i,\gamma_j)}=\prod_i \mathrm{e}\,(x_{i4}/2^{n_i})^{C^*(\gamma_i)}\prod_{i<j}\mathrm{e}\,(x_{i4}x_{j4}/2)^{C_*(\gamma_i,\gamma_j)}.$$

Here $\prod_{p'}$ *extends over all primes* p' $(\neq p, 2)$ *dividing* f.

C. The left-hand side in (i *a*), (ii *a*) *can be replaced by*

$$\prod_{i<j}\{[w(\psi_i^{x_{jp}}\psi_j^{-x_{ip}})]\,(p)\}^{C_*(\gamma_i,\gamma_j)}.$$

Corollary. *If* K *is the union of quadratic fields, and if for* $i=1,\ldots,m$, $\mathrm{P}_{\phi_i}=\mathrm{P}_{\psi_i}=\mathrm{P}(\sqrt{d_i})$ *then a necessary and sufficient condition for an element* $\bar{c}$ *of* $\overline{F}(\Gamma, E)$ *to lie in* $A(\mathrm{K})$ *is that the invariants of* $\bar{c}$ *satisfy the following conditions*:

$$(\mathrm{iv})\ \prod_{i<j}\left(\frac{d_i, d_j}{p}\right)^{C_*(\gamma_i,\gamma_j)}\prod_{i=1}^{m}\left(\frac{-1, d_i}{p}\right)^{C^*(\gamma_i)}=1,\quad \text{for all prime divisors } p.$$

Proof of the corollary. If p is non-ramified in K, then each of the symbols $(a, b/p)$ involved takes value 1, and so the condition imposed is non-trivial only for the ramified finite prime divisors and for p_∞. For p_∞ the criterion can be deduced either by the product formula of the norm residue symbol—and so the equation for p_∞ can be omitted as depending on the ones for finite p, or alternatively this equation can also be deduced directly in analogy to the methods used in proving theorem 6. Finally, if $p \mid f$, we can verify (iv) from, for example, B (ii *a*), (iii *a*) using the explicit definition of the Hilbert symbol in terms of residue characters and taking d_i as the discriminant of $\mathrm{P}(\sqrt{d_i})$.

If we take in the corollary $m=2$, $C^*(\gamma_1,\gamma_2)=C^*(\gamma_1)=C^*(\gamma_2)=1$ we obtain a criterion for K to have an extension with quaternion group which was first proved by Reichardt (1936).

Proof of theorem 7. Let for all p dividing f, $\omega_p^*=(p, \mathrm{K}^*/p)$, $\omega_p=(p, \mathrm{K}/p)$. By (9·3), (9·4), we have for $p\neq 2$,

$$\omega_p^*\equiv\prod_{q(\neq p)}\sigma_q^{*-[q,p]}\quad(\mathrm{mod}\ [\sigma_p^*]),$$

using the product formula for the norm residue symbol. Hence

$$\omega_p\equiv\prod_{q(\neq p)}\sigma_q^{-[q,p]}\quad(\mathrm{mod}\ [\sigma_p])\tag{9·9}$$

if σ_p is the coset of σ_p^* in Γ. On the other hand, $(2, \mathrm{P}(\sqrt{-1})/2)=(2, \mathrm{P}(\sqrt{2})/2)=1$. It follows that

$$\omega_2^*\equiv\prod_{q(\neq 4,8)}\sigma_q^{*-[q,2]}\quad(\mathrm{mod}\ [\sigma_8^{*2}]),$$

whence

$$\omega_2\equiv\prod_{q(\neq 4,8)}\sigma_q^{-[q,2]}\quad(\mathrm{mod}\ [\sigma_8^2]).\tag{9·9 a}$$

From (9·9) and (9·9 *a*) we get for all $p \mid f$, and for all $q'\equiv 0\ (\mathrm{mod}\, p)$

$$c_*(\omega_p, \sigma_{q'})=\prod_q c_*(\sigma_q, \sigma_{q'})^{-[q,p]},\tag{9·10}$$

the product extending over all q prime to p. Next observe that by (9·6), (9·7), for all i, q

$$\phi_i(\sigma_q) = \phi_i(\prod_j \gamma_j^{x_{jq}})$$

and so for all q

$$\sigma_q = \prod_j \gamma_j^{x_{jq}}. \tag{9·11}$$

Applying (2·8), (9·10), (9·11) we express $c_*(\omega_p, \sigma_{q'})$, $c^*(\sigma_q)$ in terms of the elements $c_*(\gamma_i, \gamma_j)$, $c^*(\gamma_i)$, and use Artin's reciprocity mapping. Theorem 7(A) is then seen to be equivalent to theorem 6. The detailed calculations are omitted.

For theorem 7(B) we observe that by (9·4)

$$\chi_q(p) = \mathrm{e}([q,p]/l) \tag{9·12}$$

whenever $(q,p) = 1$. Also by (9·5), (9·6)

$$w\psi_i = \prod_q \chi_q^{x_{iq}} \quad (i = 1, \ldots, m) \tag{9·13}$$

whence $\prod_{p'(\neq p)} w_{p'}\psi_i = \prod_{(q,p)=1} \chi_q^{x_{iq}}$. Using (9·2), (9·8), (9·12), (9·13), criterion B is seen to be equivalent with criterion A. Apart from C—to which we shall return below—theorem 7 has thus been established.

Procedure for computing $A(\mathrm{K})$. Choose a basis $[\phi_1, \ldots, \phi_m]$ of $\Phi(\mathrm{K}/\mathrm{P})$, so that order $\phi_{i+1} \leqq$ order ϕ_i. Then Γ has a basis $\mathfrak{g}$ satisfying (9·1); the elements of $\mathfrak{g}$ can of course be considered as classes mod f^*. Select for each q a rational number a_q as follows: (i) a_q is a lth power non-residue mod q, if $q = p \equiv 1 \pmod{l}$, and mod q^2, if $q = l \neq 2$; $a_4 \equiv -1$, $a_8 \equiv 5 \pmod{8}$, (ii) $a_q \equiv 1 \pmod{f^{*(q)}}$, where $f^{*(q)}$ is the greatest divisor of f^* prime to q. Then one can find integers x_{iq} satisfying $w\phi_i(a_q) = \mathrm{e}(x_{iq}/l^{n_i})$, if $l^{n_i} =$ order ϕ_i. Put $\phi_i^{l^{n_i-1}} = \psi_i$. For each solution $[C^*(\gamma_i), C_*(\gamma_i, \gamma_j)]$ of (ia) to (iii$a$) one can construct a factor system c, using (9·8) and (2·8). These factor systems then form a complete set of representatives of $A(\mathrm{K})$, and at the same time form a group—which thus is an explicit representation of $A(\mathrm{K})$.

It remains to discuss the significance of the character products and numerical exponents occurring in theorem 7. Let $\overline{\mathrm{X}}_q$ be the group of residue characters of l-power order, which are defined mod p, if $q = p \equiv 1 \pmod{l}$, and mod l^{s_l+1}, if $q = l \neq 2$; $\overline{\mathrm{X}}_4$ is the group of residue characters mod 4, and $\overline{\mathrm{X}}_8$ the group of residue characters χ mod 2^{s_2+2} with $\chi(-1) = 1$. Then $w\Phi(\mathrm{K}^*/\mathrm{P})$ is the direct product of the groups $\overline{\mathrm{X}}_q$. The $\overline{\mathrm{X}}_q$ components of $w\Phi(\mathrm{K}/\mathrm{P})$ form a subgroup X_q of $\overline{\mathrm{X}}_q$.

Denote† the maximal subfield of K, whose Galois group has exponent dividing l by $\mathrm{K}^{(l)}$, so that $\Phi_{(l)}(\mathrm{K}/\mathrm{P}) = \Phi(\mathrm{K}^{(l)}/\mathrm{P})$. Let $w\Phi(\mathrm{K}_q/\mathrm{P})$, $w\Phi(\mathrm{K}_q^{(l)}/\mathrm{P})$ be the maximal subgroups of $w\Phi(\mathrm{K}/\mathrm{P})$, respectively $w\Phi(\mathrm{K}^{(l)}/\mathrm{P})$, of characters whose $\overline{\mathrm{X}}_q$ component is 1. Then K_q is the invariant field of $[\sigma_q]$, and $\mathrm{K}_q^{(l)} = \mathrm{K}_q \cap \mathrm{K}^{(l)}$. The inertia fields of an odd prime p in K, and $\mathrm{K}^{(l)}$ are the fields K_p, $\mathrm{K}_p^{(l)}$, and the inertia fields of 2 in K, and $\mathrm{K}^{(2)}$ are the fields $\mathrm{K}_4 \cap \mathrm{K}_8$, respectively $\mathrm{K}_4^{(2)} \cap \mathrm{K}_8^{(2)}$.

One can clearly assume $y_{iq} \not\equiv 0$, $[q,p] \not\equiv 0 \pmod{l^{s_q+1}}$, $x_{iq} \not\equiv 0 \pmod{l^{n_i+1}}$. The order l^{s_q} of $\overline{\mathrm{X}}_q$ is an invariant of $\Phi(\mathrm{K}/\mathrm{P})$, and so is the sequence $[l^{n_1}, \ldots, l^{n_m}]$ $(n_i \geqq n_{i+1})$. On the other hand, a change in the particular generator $\bar{\chi}_q$ of $\overline{\mathrm{X}}_q$ selected will amount to a substitution

$$(a) \quad x_{iq} \to x_{iq} r_q, \quad y_{iq} \to y_{iq} r_q, \quad r_q[q, p] \to [q, p] \quad ((r_q, l) = 1),$$

† The symbol $\mathrm{K}^{(2)}$ has here a different meaning from that in §8. In neither place does the symbol appear in the final results and so no confusion should arise.

while a change of basis of $\Phi(\mathrm{K}/\mathrm{P})$ leads to a substitution

$$(b)\qquad \left.\begin{matrix} x_{iq} \\ y_{iq} \end{matrix}\right\} \rightarrow \sum_j a_{ij} \left\{\begin{matrix} x_{jq}, \\ y_{jq} \end{matrix}\right. \qquad [q,p] \rightarrow [q,p],$$

with (a_{ij}) as a unimodular matrix with respect to the ring L of l-adic integers.

We consider the matrices

$$X = (x_{iq})_{i,q}, \quad Y = (y_{iq})_{i,q},$$

the column indices q being ordered in a given manner, and for each subsequence $[q_1, \ldots, q_r]$ of the sequence of column indices, also the matrices

$$X(q_1, \ldots, q_r), \quad Y(q_1, \ldots, q_r)$$

consisting of the columns $q_1, \ldots, q_r$ of X, and of Y, respectively. One has then without loss of generality

$$X(q_1, \ldots, q_r) \operatorname{diag}(l^{s_{q_1}}, \ldots, l^{s_{q_r}}) = \operatorname{diag}(l^{n_1}, \ldots, l^{n_m})\, Y(q_1, \ldots, q_r).$$

The rank mod l, and the elementary divisors in L of these matrices are invariants of the substitutions (a), (b).

The immediate and obvious invariant characterization of the matrices Y and X is in terms of the group invariants of $\Phi(\mathrm{K}^*/\mathrm{P})/\Phi(\mathrm{K}/\mathrm{P})$ and of $\Phi_{(l)}(\mathrm{K}^*/\mathrm{P})/\Phi_{(l)}(\mathrm{K}/\mathrm{P})$. More precisely these group invariants are the elementary divisors, in the ring L of l-adic integers, of the matrices

$$\begin{bmatrix} Y \\ (\operatorname{diag} l^{s_q})_q \end{bmatrix}, \quad \begin{bmatrix} X \\ (\operatorname{diag} l)_q \end{bmatrix},$$

respectively (by (9·5), (9·13)). We shall, however, mainly be concerned with certain submatrices of X and Y. Use will be made of the following two results.

I. *The elementary divisor in L of the column matrix $Y(q)$ is the order ideal of* $\overline{\mathrm{X}}_q/\mathrm{X}_q$ (*by* (9·5)).

II. *The elementary divisors in L of*

$$[X(q_1, \ldots, q_r) \mid \operatorname{diag} l]$$

are the group invariants of $\Phi_{(l)}(\mathrm{K}_{q_1} \cap \ldots \cap \mathrm{K}_{q_r}/\mathrm{P})$. *The rank* mod l *of* $X(q_1, \ldots, q_r)$ *is the l-dimension of* $\Phi_{(l)}(\mathrm{K}/\mathrm{P})/\Phi_{(l)}(\mathrm{K}_{q_1} \cap \ldots \cap \mathrm{K}_{q_r}/\mathrm{P})$ (*by* (9·11)).

The criterion for $A(\mathrm{K})$ in theorem 7 is stated in terms of a system of equations for the unknowns $C^*(\gamma_i)$, $C_*(\gamma_i, \gamma_j)$, respectively $c^*(\gamma_i)$, $c_*(\gamma_i, \gamma_j)$. There is one equation for each prime divisor p of f, with the convention that for $p = l \neq 2$ the equation is trivial. Accordingly one can refer to the p-equation, or for $p \mid q$, to the q-equation of the system. Our aim is to investigate what may be called the 'system of coefficients' of the system of equations.† As seen from A the coefficients are functions of the x_{iq}, the $[q,p]$, and the group invariant $[l^{n_1}, \ldots, l^{n_m}]$.

First consider the left-hand sides. By inspection of (ia) to (iii$a$) we see that, in the first place, these depend solely on $\Phi_{(l)}(\mathrm{K}/\mathrm{P})$ and not on the whole group $\Phi(\mathrm{K}/\mathrm{P})$. In fact the exponents x_{iq} are to be taken mod l, but they are determined mod l by (9·13), i.e. by the basis $[\psi_1, \ldots, \psi_m]$ of $\Phi_{(l)}(\mathrm{K}/\mathrm{P})$. Next we note that the left-hand sides are essentially determined by the mutual congruence behaviour of the primes dividing f. In fact the ideal

† One can in fact write the criterion of theorem 7 as a system of linear congruences.

$([q,p],l)$ is invariant under substitutions (a) and (b); also $([q,p],l) = (1)$ or $= (l)$, and the latter is the case if and only if (i) p is lth power residue mod q, if $q \equiv 1 \pmod{l}$, or $q = 4$, (ii) p is lth power residue mod l^2, if $q = l \neq 2$, (iii) $p \equiv \pm 1 \pmod{8}$, if $q = 8$. Thus if p is an lth power residue mod $f^{*(p)}$, where $(f^{*(p)}, p) = 1$, $f^* = f^{*(p)} p^r$, then the left-hand side of the p-equation is trivial, i.e. takes value 1 identically; moreover, if this is true for all p, then when $l \neq 2$, the invariants $c_*(\gamma_i, \gamma_j)$ can be chosen arbitrarily, and the invariants $c^*(\gamma_i)$ have to be chosen so that the right-hand sides take value 1.

Now use criterion II, for $r = 1, 2$. The rank mod l of $X(q)$ is zero, i.e. $x_{iq} \equiv 0 \pmod{l}$ for all i, if and only if $K_q^{(l)} = K^{(l)}$. Thus whenever $K_q^{(l)} = K^{(l)}$, the left-hand side of the q-equation will take value 1 identically, and the 'q-term' on the left of any other equation can be omitted. Next consider the expressions $x_{iq} x_{jq'} - x_{jq} x_{iq'}$ occurring in (i) to (iii). These are the subdeterminants of order 2 in $X(q, q')$. By II they will all vanish, if and only if $\Gamma(K^{(l)}/K_q^{(l)})$, $\Gamma(K^{(l)}/K_{q'}^{(l)})$ are not independent subgroups of $\Gamma(K^{(l)}/P)$, i.e. if and only if $K_q^{(l)} \subseteq K_{q'}^{(l)}$, or $K_{q'}^{(l)} \subseteq K_q^{(l)}$. Thus in this case the left-hand sides are in fact independent of what one may call the mutual congruence behaviour of q and q'. In particular if $x_{sq} \not\equiv 0$, $x_{tq'} \not\equiv 0 \pmod{l}$ for some s, t, i.e. if $X(q)$, $X(q')$ have rank 1 mod l, then $x_{iq} x_{jq'} - x_{jq} x_{iq'} \equiv 0 \pmod{l}$, all i, j, if and only if $K_q^{(l)} = K_{q'}^{(l)}$. Restricting ourselves for simplicity's sake to the case $(f, 2) = 1$ we can conclude:† the left-hand sides depend on the mutual congruence behaviour of pairs (p, p') of distinct prime divisors of f—but only if both p and p' are ramified in $K^{(l)}$, and if the inertia fields $K_p^{(l)}$, $K_{p'}^{(l)}$ do not coincide.‡

The $\overline{X}_q$ component of $w(\psi_i^{x_{jq}} \psi_j^{-x_{iq}})$ is 1. Hence $\psi_i^{x_{jq}} \psi_j^{-x_{iq}} \in \Phi(K_q^{(l)}/P)$. It follows that if $q = p$ is an odd prime, then $w_p(\psi_i^{x_{jq}} \psi_j^{-x_{iq}}) = 1$, and so $w(\psi_i^{x_{jp}} \psi_j^{-x_{ip}}) = \prod_{p'(\neq p)} w_{p'}(\psi_i^{x_{jp}} \psi_j^{-x_{ip}})$. This justifies theorem 3 (C). Assume now that the rank mod l of $X(q)$ is not zero. Then without loss of generality one may take $x_{1q} = 1$. It follows that $\psi_i^1 \psi_1^{-x_{iq}}$ is a basis of $\Phi(K_q^{(l)}/P)$. Thus the characters $\psi_i^{x_{jq}} \psi_j^{-x_{iq}}$ generate $\Phi(K_q^{(l)}/P)$ whenever $K_q^{(l)} \neq K$.

We now turn to the right-hand sides, where we shall consider the 'coefficients' $e(x_{ip}(p-1)/l^{n_i+1})$. Neglecting the additional factor occurring in the case $l = 2$, the right-hand sides can be written in the form $e\{(1/l)\, \Sigma x_{ip}(p-1)\, C^*(\gamma_i)/l^{n_i}\}$, where $p \equiv 1 \pmod{l}$. But one can assume $x_{ip}/l^{n_i} = y_{ip}/l^{s_p}$; also $(p-1)/l^{s_p}$ is an l-adic unit. Thus apart from unit factors in L the column matrix $(x_{ip}(p-1)/l^{n_i})$ coincides with the matrix $Y(p)$. Hence by I the right-hand side of the p-equation essentially depends on the group index $(\overline{X}_p : X_p)$. A necessary and sufficient condition that the right-hand side of the p-equation be trivial, i.e. have identically value 1, is that $(\overline{X}_p : X_p) \equiv 0 \pmod{l}$, i.e. that p should not attain the 'maximal possible' order of ramification in K. A similar interpretation also applies to (iii), respectively (iii$a$).

Let now $x_{ip}/l^{n_i} = z_{ip}/l^{n_{i,p}}$, $(z_{ip}, l) = 1$; here $l^{n_{i,p}}$ is the order of $\phi_i \bmod \Phi(K_p/P)$. Then $e(x_{ip}(p-1)/l^{n_i+1}) = e((p-1)/l^{n_{i,p}+1})^{z_{ip}}$, where $p \equiv 1 \pmod{l^{n_{i,p}}}$. We now observe that the function θ_{lm} defined on the group of rationals $a \equiv 1 \pmod{l^m}$ by $\theta_{lm}(a) = e((a-1)/l^{m+1})$ is a character of that group mod l^{m+1}. If in particular $n_i = 1$, all i then the right-hand side will appear in the simple form $(\theta_l(p))^{\sum_i x_{ip} C^*(\gamma_i)}$.

† A similar statement can of course be formulated in the general case.

‡ Here only the ranks mod l of $X(q_1, \ldots, q_r)$ for $r = 1, 2$ have been dealt with. It can be shown that the ranks mod l for $r > 2$ also reflect certain significant properties of the system of equations. A detailed statement however would already for $r = 3$ have to cope with a fairly complicated situation.

10. Description of the character group $\Phi(\overline{\Lambda}/K)$

In the present section theorems 5 and 6 will be used to express the structure of the group $\Phi^*(\overline{\Lambda}/K)$ in rational terms and to give a description of the group $\Phi(\overline{\Lambda}/K)$, i.e of $\mathfrak{C}(K/P)$. For this purpose it is convenient to introduce the group $\Theta(K/P)$ of genus characters of order l in K, well known in the theory of absolutely Abelian fields. In terms of ideal classes $\Theta(K/P)$ is simply the group of characters of order l of the genus group mod 1, if $(f, 2) = 1$. In terms of idèle classes $\Theta(K/P)$ is the subgroup of $\Phi(K)$ which is the character group of $J_K/L_K U_K$. Here J_K—as before—is the idèle group of K; L_K was defined in § 4, and U_K is the group of unit idèles which are positive at all real infinite prime divisors and in the case when $2 \mid f$, are squares at the prime divisors above 2.

In keeping with our programme we shall want to characterize $\Theta(K/P)$ rationally. That this is possible is a classical result. Let for each character $\psi \in \Psi^*_{(l)}(K/P) = \Phi_{(l)}(K^*/P)$, $s\psi$ be its restriction to the idèle norms of K in P. Now define a character ϕ on J_K by

$$\phi(\mathfrak{A}) = [s\psi]\,(N_{K/P}\,\mathfrak{A}). \tag{10·1}$$

Then $\phi \in \Theta(K/P)$ and the mapping $s\psi \to \phi$ sets up an isomorphism of $s\Phi_{(l)}(K^*/P)$ onto $\Theta(K/P)$.

From (10·1) it follows that $\phi = R\psi$, $\psi \in \Psi^*(K/P)$. Assume conversely that $\phi \in \Phi(\overline{\Lambda}/K)$, $\phi = R\psi'$, $\psi' \in \Psi^*(K/P)$. Then $\psi' = \psi\psi''$, where $\psi \in \Psi^*_{(l)}(K/P)$, $\psi'' \in \Phi(K/P)$, and thus $\phi = R\psi$. But then ϕ, ψ satisfy (10·1). We have seen that

$$\Theta(K/P) = R\Psi^*(K/P). \tag{10·2}$$

By (10·2) and theorem 5 we now get

Theorem 8. *$\Theta(K/P)$ is a subgroup of $\Phi^*(\overline{\Lambda}/K)$ and is the kernel of u^*. $\Phi^*(\overline{\Lambda}/K)$ is the direct product of $\Theta(K/P)$ and of a group $\overline{\Theta}$ which contains for every element $\bar{c} \in A(K)$ a unique character $\theta_{\bar{c}}$ such that $u\theta_{\bar{c}} = \bar{c}$.*

For the second part of the theorem we only have to note that every subgroup of the elementary Abelian group $\Phi^*(\overline{\Lambda}/K)$ is a direct component.

As the groups $\Theta(K/P)$ and $A(K)$ are determinable in the rational field, theorem 8 provides a rational determination of $\Phi^*(\overline{\Lambda}/K)$, and thus by theorem 5 also of $\Phi(\overline{\Lambda}/K)$. Every character ϕ in $\Phi(\overline{\Lambda}/K)$ has a unique 'parametric' representation $\phi = \theta.\theta_{\bar{c}}.R\psi$, with $\theta \in \Theta(K/P)$, $\psi \in \Psi_*(K/P)$, $\theta_{\bar{c}} \in \overline{\Theta}$, $\bar{c} = u\phi$; also ϕ has a representation $\phi = \theta_{\bar{c}}.R\psi'$, with $\psi' \in \Psi(K/P)$, and ψ unique mod $\Phi(K/P)$. It should, however, be noted that the group $\overline{\Theta}$ in theorem 8 is not in general unique. There is in fact no canonical procedure of singling out such a group of representatives of $A(K)$ in a unique manner.

Next an explicit description of the group $\Phi(\overline{\Lambda}/K)$ will be given, not using the subgroup $\overline{\Theta}$, but solely the rationally determined invariants $\Theta(K/P)$, $A(K)$, and $\Psi_*(K/P)$. At each step the conditions in terms of these invariants will be interpreted as conditions on the class-group structure in K. Let then ψ be a rational idèle class character of order l not ramified at any prime divisor of f, and let $\bar{c}$ be an element of $A(K)$, i.e. a solution of the system of equations in theorems 6 or 7. Then there exists a character $\phi \in \Phi(\overline{\Lambda}/K)$, such that

(i) $u\phi = \bar{c}$.

(ii) $\phi.R\psi^{-1}$ is non-ramified at all finite prime divisors of K, non-ramified in K/P.

Condition (i) is equivalent to a set of equations

$$\phi(\mathfrak{A}_\gamma) = c^*(\gamma), \quad \phi(\mathfrak{B}_{\delta,\gamma}) = c_*(\delta,\gamma)$$

on L_{K}, as set out in detail in theorem 3. Condition (ii) is equivalent to the set of equations

$$\phi(\mathfrak{A}) = \psi(N_{\mathrm{K/P}}\mathfrak{A})$$

for all unit idèles $\mathfrak{A}$, whose components at the finite ramified prime divisors in K are 1. Also if ϕ satisfies (i) to (ii), then so does ϕ_1, if and only if

(iii) $\phi = \phi'\phi_1$, $\phi' \in \Theta(\mathrm{K/P})$.

Condition (iii) is equivalent to $\qquad \phi(\mathfrak{A}) = \phi_1(\mathfrak{A})$

if $\mathfrak{A} \in L_{\mathrm{K}}U_{\mathrm{K}}$. Finally, every character ϕ_1 in $\Phi(\overline{\Lambda}/\mathrm{K})$ is obtained in this manner, i.e. by (i) to (iii).

The stated results, and the description of $\Phi(\overline{\Lambda}/\mathrm{K})$ still leave the problem of determining the local components of characters from their invariants. This will be dealt with in § 12.

In conclusion a special case will briefly be discussed. By corollary 2 of theorem 5 the mapping u^* is an isomorphism if and only if

$$\Psi^*(\mathrm{K/P}) = \Phi(\mathrm{K/P}). \tag{10·3}$$

Now $\Psi^*(\mathrm{K/P}) = \Psi^*_{(l)}(\mathrm{K/P}).\Phi(\mathrm{K/P})$; also $\Psi^*_{(l)}(\mathrm{K/P}) = \Phi_{(l)}(\mathrm{K^*/P})$. Thus (10·3) is equivalent with

$$\Phi_{(l)}(\mathrm{K^*/P}) = \Phi_{(l)}(\mathrm{K/P}). \tag{10·4}$$

Thus (10·3) holds if and only if $\mathrm{K}^{(l)}$ is its own genus field, and in addition $\mathrm{P}(\sqrt{-1}, \sqrt{2}) \subseteq \mathrm{K}^{(l)}$ whenever $l = 2 \mid f$. In this case then every character ϕ in $\Phi^*(\overline{\Lambda}/\mathrm{K})$ is uniquely determined by $u\phi$, the group $\Theta(\mathrm{K/P}) = 1$, and $\overline{\Theta}$ is the unique group $\Phi^*(\overline{\Lambda}/\mathrm{K})$. Conditions (i), (ii) in the description of $\Phi(\overline{\Lambda}/\mathrm{K})$ determine ϕ uniquely.

11. Absolutely Abelian extensions

The present section will be concerned with the subset of $\mathfrak{C}(\mathrm{K/P})$ of fields which are Abelian over P, and the corresponding group $\Phi_A(\overline{\Lambda}/\mathrm{K})$ consisting of all characters ϕ in $\Phi(\overline{\Lambda}/\mathrm{K})$ for which K_ϕ is Abelian. This set of fields can of course be determined by direct application of the fundamental theorem of class-field theory. Our aim, however, is to show how the structure of $\Phi_A(\overline{\Lambda}/\mathrm{K})$ and the embedding of this group in $\Phi(\overline{\Lambda}/\mathrm{K})$ is described in terms of the theory developed here.

Obviously one has $\Phi_A(\overline{\Lambda}/\mathrm{K}) = (R\Phi(\mathrm{P})) \cap \Phi(\overline{\Lambda}/\mathrm{K})$; the question then arises how to characterize rationally the subgroup of $\Phi(\mathrm{P})$ of elements ϕ for which $R\phi \in \Phi(\overline{\Lambda}/\mathrm{K})$. For this purpose define a subgroup $\overline{\Psi}(\mathrm{K/P})$ of $\Phi(\mathrm{P})$, as the group of characters ϕ, such that $\phi^l \in \Phi(\mathrm{K/P})$. It will then be shown that this is the required group.

We have seen in § 2 that to every class $\bar{c}$ of $\overline{F}(\Gamma, E)$ there corresponds a unique commutator factor system c_*. The homomorphism $\bar{c} \to c_*$ of $\overline{F}(\Gamma, E)$ onto $C(\Gamma, E)$ will here be denoted by h, and we write $hA(\mathrm{K}) = C(\mathrm{K})$. We saw in § 4 (cf. (4·8)) that the kernel of h is the subgroup $\overline{F}_A(\Gamma, E)$ of factor-system classes which are operative for Abelian extensions of E by Γ. Next we recall from § 2 that to each class $\bar{c}$ of $\overline{F}_A(\Gamma, E)$ there corresponds a power-factor system c^* in $P(\Gamma, E)$ with $c^*(1) = 1$. Denote the mapping $\bar{c} \to c^*$ of $\overline{F}_A(\Gamma, E)$ into $P(\Gamma, E)$ by g and write $g(\overline{F}_A(\Gamma, E) \cap A(\mathrm{K})) = P(\mathrm{K})$.

Assume that $\bar{c}_1, \bar{c}_2 \in \overline{F}_A(\Gamma, E)$, and that $g\bar{c}_1 = g\bar{c}_2$. We also have $h\bar{c}_1 = h\bar{c}_2 = 1$. But the mapping $\bar{c} \rightarrow (c_*, c^*)$ is biunique, and so $\bar{c}_1 = \bar{c}_2$. It follows that g is an isomorphism of $\overline{F}_A(\Gamma, E)$ into $P(\Gamma, E)$. Let now $c^* = g\bar{c}$, $\bar{c} \in \overline{F}_A(\Gamma, E)$. If $\gamma \in \Gamma$, $\gamma^l \neq 1$, then $c^*(\gamma) = c^*(\gamma^l)$, as can easily be verified. Thus c^* is completely determined by its values on $\Gamma_{(l)}$, the subgroup of Γ, of elements γ with $\gamma^l = 1$. Write for all $\gamma \in \Gamma_{(l)}$

$$\phi(\gamma) = c^*(\gamma)^{l/n_\gamma}, \tag{11·1}$$

n_γ denoting the order of γ. Then by direct calculation we verify the formula

$$\phi(\gamma_1 \gamma_2) = \phi(\gamma_1)\,\phi(\gamma_2).$$

ϕ is thus a character of $\Gamma_{(l)}$. Also $\phi = 1$, if and only if $\bar{c} = 1$. It follows that the mapping $\bar{c} \rightarrow \phi$ is an isomorphism of $\overline{F}_A(\Gamma, E)$ into the character group $\Phi(\Gamma_{(l)})$ of $\Gamma_{(l)}$. Assume conversely that $\phi \in \Phi(\Gamma_{(l)})$. Let $\mathfrak{g} = [\gamma_1, \ldots, \gamma_m]$ be a basis of Γ, and let for $i = 1, \ldots, m$, $\gamma'_i = \gamma_i^{ln_i - 1} \neq 1$, $\gamma'_i \in \Gamma_{(l)}$. Put $c^*(\gamma_i) = \phi(\gamma'_i)$, for $i = 1, \ldots, m$, and $c_*(\gamma_i, \gamma_j) = 1$, and construct a factor system c in $F_{\mathfrak{g}}(\Gamma, E)$ by (2·8). Then $\bar{c} \in \overline{F}_A(\Gamma, E)$, and for $g\bar{c} = c^*$ (11·1) will hold. Using (11·1) one may thus identify $g\overline{F}_A(\Gamma, E)$ with $\Phi(\Gamma_{(l)})$. On the other hand, the restriction of characters of $\Phi(\mathrm{K}/\mathrm{P}) = \Phi(\Gamma)$ to $\Gamma_{(l)}$ has kernel $\Phi^l(\mathrm{K}/\mathrm{P})$, and one may thus identify

$$\Phi(\Gamma_{(l)}) = \Phi(\mathrm{K}/\mathrm{P})/\Phi^l(\mathrm{K}/\mathrm{P}).$$

g will then be considered as an isomorphism of $\overline{F}_A(\Gamma, E)$ onto $\Phi(\mathrm{K}/\mathrm{P})/\Phi^l(\mathrm{K}/\mathrm{P})$. It remains to find the subgroup $P(\mathrm{K})$.

THEOREM 9

(i) *$R\overline{\Psi}^l(\mathrm{K}/\mathrm{P}) = \Phi_A(\overline{\Lambda}/\mathrm{K})$, and $\overline{\Psi}^l(\mathrm{K}/\mathrm{P})$ is the inverse image of $\Phi_A(\overline{\Lambda}/\mathrm{K})$ under R. The sequence*† *of homomorphisms*

$$1 \rightarrow \Phi(\mathrm{K}/\mathrm{P}) \rightarrow \overline{\Psi}^l(\mathrm{K}/\mathrm{P}) \xrightarrow{R} \Phi(\overline{\Lambda}/\mathrm{K}) \xrightarrow{hu} C(\mathrm{K}) \rightarrow 1$$

is exact.

(ii) *If $\psi \in \overline{\Psi}^l(\mathrm{K}/\mathrm{P})$, $guR\psi = c^*$ then $c^*(1) = 1$, and for all*‡ *$\gamma \in \Gamma$, $\gamma \neq 1$, $c^*(\gamma) = \psi^{n_\gamma}(\gamma)$, where n_γ is the order of γ in Γ. $P(\mathrm{K})$ is the subgroup $\overline{\Psi}^l(\mathrm{K}/\mathrm{P})/\Phi^l(\mathrm{K}/\mathrm{P})$ of $\Phi(\mathrm{K}/\mathrm{P})/\Phi^l(\mathrm{K}/\mathrm{P})$, and the sequence of homomorphisms*

$$1 \rightarrow \Psi^l(\mathrm{K}/\mathrm{P}) \rightarrow \overline{\Psi}^l(\mathrm{K}/\mathrm{P}) \xrightarrow{guR} P(\mathrm{K}) \rightarrow 1$$

is exact.

Proof

(i) As in theorem 1 we find that $\Phi(\mathrm{K}/\mathrm{P})$ is the kernel of R. As $\Phi(\mathrm{K}/\mathrm{P}) \subseteq \overline{\Psi}^l(\mathrm{K}/\mathrm{P})$, this and the formula $R\overline{\Psi}^l(\mathrm{K}/\mathrm{P}) = \Phi_A(\overline{\Lambda}/\mathrm{K})$ imply that $\overline{\Psi}^l(\mathrm{K}/\mathrm{P})$ is the required inverse image. The kernel of h in $\overline{F}(\Gamma, E)$ is $\overline{F}_A(\Gamma, E)$. Hence $hu\phi = 1$, if and only if $u\phi \in \overline{F}_A(\Gamma, E)$, i.e. $\phi \in \Phi_A(\overline{\Lambda}/\mathrm{K})$. It then only remains to establish the first formula in (i).

Assume that $\phi \in \Phi_A(\overline{\Lambda}/\mathrm{K})$. Then $\phi = R\psi$, $\psi \in \Phi(\mathrm{P})$. But $\phi^l = 1$, i.e. $R\psi^l = 1$, and so ψ^l lies in the kernel $\Phi(\mathrm{K}/\mathrm{P})$ of R; hence $\psi \in \overline{\Psi}^l(\mathrm{K}/\mathrm{P})$. Conversely assume that $\psi \in \overline{\Psi}^l(\mathrm{K}/\mathrm{P})$, $R\psi = \phi$. Then $\psi^l \in \Phi(\mathrm{K}/\mathrm{P})$, i.e. $\phi^l = 1$. Thus $(\mathrm{K}_\phi : \mathrm{K}) \mid l$. But K_ϕ is Abelian, and hence $\mathrm{K}_\phi \in \mathfrak{C}(\mathrm{K}/\mathrm{P})$, $\phi \in \Phi_A(\overline{\Lambda}/\mathrm{K})$.

(ii) Let $\psi \in \overline{\Psi}^l(\mathrm{K}/\mathrm{P})$, $\phi = R\psi$, $\mathrm{K}_\phi = \Lambda$, $gu\phi = c^*$. Let a be a factor system in the operative class for $\Lambda/\mathrm{K}/\mathrm{P}$; then if $\gamma \in \Gamma$, $\gamma \neq 1$,

$$\phi(a^*(\gamma)) = c^*(\gamma). \tag{11·2}$$

† $\Phi(\overline{\mathrm{K}/\mathrm{P}}) \rightarrow \Psi^l(\mathrm{K}/\mathrm{P})$ in (i), $\Psi^l(\overline{\mathrm{K}/\mathrm{P}}) \rightarrow \Psi^l(\mathrm{K}/\mathrm{P})$ in (ii) are the injection mappings.

‡ Note that $n_\gamma \equiv 0 \pmod{l}$, and that therefore $\psi^{n_\gamma} \in \Phi(\mathrm{K}/\mathrm{P})$, so that $\psi^{n_\gamma}(\gamma)$ is defined.

Now if $\bar{\gamma}$ is any representative of γ in $\Gamma(\Lambda/\mathrm{P})$, and if n_γ is the order of γ in Γ, then

$$\bar{\gamma}^{n_\gamma} = a^*(\gamma).$$

Hence $\phi(a^*(\gamma)) = \phi(\bar{\gamma}^{n_\gamma})$; also $\phi(\gamma') = \psi(\gamma')$ for all $\gamma' \in \Gamma(\Lambda/\mathrm{K})$. Therefore

$$\psi(\bar{\gamma}^{n_\gamma}) = \phi(a^*(\gamma)). \tag{11·3}$$

Now $\psi(\bar{\gamma}^{n_\gamma}) = \psi^{n_\gamma}(\bar{\gamma})$. But $\psi^{n_\gamma} \in \Phi(\mathrm{K}/\mathrm{P})$, and so $\psi^{n_\gamma}(\bar{\gamma})$ solely depends on $\bar{\gamma} \bmod \Gamma(\Lambda/\mathrm{K})$, i.e. on γ. Thus $\psi(\bar{\gamma}^{n_\gamma}) = \psi^{n_\gamma}(\gamma)$. By (11·2), (11·3) we obtain the required formula

$$c^*(\gamma) = \psi^{n_\gamma}(\gamma). \tag{11·4}$$

Restrict now the argument γ to $\Gamma_{(l)}$. Then if ϕ' is given by (11·1) we get from (11·4) that

$$\phi'(\gamma) = \psi^l(\gamma)$$

for all $\gamma \in \Gamma_{(l)}$, including of course $\gamma = 1$. Thus $\phi' \equiv \psi^l \pmod{\Phi^l(\mathrm{K}/\mathrm{P})}$. It follows now that $P(\mathrm{K}) = \overline{\Psi}^l(\mathrm{K}/\mathrm{P})/\Phi^l(\mathrm{K}/\mathrm{P})$.

We finally observe that g is an isomorphism, so that $guR\psi = 1$ if and only if $uR\psi = 1$, hence by theorem 1 if and only if $\psi \in \Psi(\mathrm{K}/\mathrm{P})$. Therefore the sequence in (ii) is exact.

12. Local properties

The principal aim of this section is the study of the relation between the 'global' invariants of $\mathfrak{C}(\mathrm{K}/\mathrm{P})$ and certain local invariants, using the formal theory of § 6. A number of results on the invariants of $\mathfrak{C}(\mathrm{K}_p/\mathrm{P}_p)$, for rational prime divisors p, will be needed but no detailed account of this subject† is to be given and proofs will be omitted, whenever they could be supplied by an adaptation of the corresponding proofs for the set $\mathfrak{C}(\mathrm{K}/\mathrm{P})$. One can restrict oneself mainly to finite prime divisors, the infinite case being trivial. The prime 2 presents certain special features, which however will not be discussed here in detail.‡ Furthermore, all primes p with $(p(p-1), l) = 1$ can be excluded from consideration.

We have, in analogy to theorem 6:

I. $\bar{c}_p \in A(\mathrm{K}_p)$, *if and only if*

(i) *when* $p \equiv 1 \pmod{l}$

$$\prod_{r \bmod p-1} c_p(a, a^r) = c_p(a, p)\,(c_p(p, a))^{-1}$$

for all units a *of* P_p;

(ii) *when* $p = 2 = l$

$$\prod_{r \bmod 2} c_2(-1, (-1)^r) = c_2(5, 2)\,(c_2(2, 5))^{-1}.$$

When $p = l \neq 2$, *then* $A(\mathrm{K}_p) = \overline{F}(\Gamma_p, E)$.

For the sake of completeness we note that for the infinite prime divisor p_∞ we have $A(\mathrm{K}_\infty) = 1$; this however is only a restriction for $l = 2$; for otherwise $\Gamma_{p\infty} = 1$.

Theorem 10. *A necessary and sufficient condition for an element* $\bar{c}$ *of* $\overline{F}(\Gamma, E)$ *to lie in* $A(\mathrm{K})$ *is that* $\bar{c}_p$ *lie in* $A(\mathrm{K}_p)$ *for all finite prime divisors* p *of* f *(equivalently: for all prime divisors* p *in* P*).*

† The methods of proof and the results of the theory of $\mathfrak{C}(\mathrm{K}_p/\mathrm{P}_p)$ are in close analogy to those of the 'global' theory derived in the preceding sections. The local theory is in fact a simplified version of the global one.

‡ See the forthcoming paper on decomposition of primes in certain non-Abelian number fields.

The first version follows by comparison of I and theorem 6. But then *a fortiori*: $\bar{c}_p \in A(\mathrm{K}_p)$ for all prime divisors p in P implies $\bar{c} \in A(\mathrm{K})$, while the converse follows by theorem 4.

We now observe that the restrictive conditions on $A(\mathrm{K})$ refer solely to prime divisors p for which P_p contains the primitive lth roots of unity, i.e. to $p \equiv 1 \pmod{l}$, and to $p = 2$, if $l = 2$ (also to p_∞, if $l = 2$). We thus get by theorem 3:

Corollary. *A necessary and sufficient condition for an element $\bar{c}$ of $\bar{F}(\Gamma, E)$ to lie in $A(\mathrm{K})$ is that for all prime divisors p, of which P_p contains the primitive lth roots of unity, the element $\bar{c}_p$ of $\bar{F}(\Gamma_p, E)$ be mapped onto the unit class of $\bar{F}(\Gamma_p, V_{\mathrm{K}_p})$. Here the mapping is any homomorphism*

$$\bar{F}(\Gamma_p, E) \rightarrow \bar{F}(\Gamma_p, V_{\mathrm{K}_p})$$

induced by some isomorphism $E \rightarrow V_{\mathrm{K}_p}$ (cf. § 5).

This corollary suggests a general law not only holding when P is the rational field, but also when P is an arbitrary finite algebraic number field: $\bar{c} \in A(\mathrm{K})$, if and only if for all prime divisors $\mathfrak{p}$ such that $\mathrm{P}_\mathfrak{p}$ contains the lth roots of unity, the element $\bar{c}_\mathfrak{p}$ of $\bar{F}(\Gamma_\mathfrak{p}, E)$ falls into the unit class of $\bar{F}(\Gamma_\mathfrak{p}, V_{\mathrm{K}\mathfrak{p}})$. That this condition is necessary follows from theorems 3 and 4. For its sufficiency we should have to show (i) $\bar{c} \in A(\mathrm{K})$, if $\bar{c}_\mathfrak{p} \in A(\mathrm{K}_\mathfrak{p})$ for all $\mathfrak{p}$, (ii) $A(\mathrm{K}_\mathfrak{p}) = \bar{F}(\Gamma_\mathfrak{p}, E)$, if $\mathrm{P}_\mathfrak{p}$ does not contain the lth roots of unity. There are also other considerations supporting this conjecture. The crux of a sufficiency proof would lie in (i).

Let now T_p be the inertia group of Γ_p. Denoting the coset mod T_p of an element γ in Γ_p by $\bar{\gamma}$, the rule

$$c(\gamma_1, \gamma_2) = b(\bar{\gamma}_1, \bar{\gamma}_2)$$

associates with each element b of $F(\Gamma_p/\mathrm{T}_p, E)$ an element c of $F(\Gamma_p, E)$, and $\bar{c}$ will be the unit class of $\bar{F}(\Gamma_p, E)$, if $\bar{b}$ is the unit class of $\bar{F}(\Gamma_p/\mathrm{T}_p, E)$. It follows that the mapping $\bar{b} \rightarrow \bar{c}$ is an homomorphism f_p of $\bar{F}(\Gamma_p/\mathrm{T}_p, E)$ into $\bar{F}(\Gamma_p, E)$. It can also easily be established that—denoting the invariant field of T_p by K'_p—$f_p u_{\mathrm{K}'_p/\mathrm{P}_p} \phi = u_{\mathrm{K}_p/\mathrm{P}_p} R_{\mathrm{K}'_p/\mathrm{K}_p} \phi$, for $\phi \in \Phi(\bar{\Lambda}(\mathrm{K}'_p)/\mathrm{K}'_p)$. Write $f_p \bar{F}(\Gamma_p/\mathrm{T}_p, E) = \bar{F}_N(\Gamma_p, E)$. We shall find that

$$\bar{F}_N(\Gamma_p, E) = u_p \Phi_N(\bar{\Lambda}_p/\mathrm{K}_p), \tag{12·1}$$

where $\Phi_N(\bar{\Lambda}_p/\mathrm{K}_p)$ is the subgroup of non-ramified characters in $\Phi(\bar{\Lambda}_p/\mathrm{K}_p)$. (12·1) in particular implies

$$\bar{F}_N(\Gamma_p, E) \subseteq A(\mathrm{K}_p). \tag{12·2}$$

By the preceding remarks, (12·1) will be established once it has been shown that with K'_p in the same connotation as above,

(*a*) (12·1) holds when $\mathrm{T}_p = 1$, i.e. $\mathrm{K}'_p = \mathrm{K}_p$.

(*b*) $\exists \phi \in \Phi_N(\bar{\Lambda}(\mathrm{K}'_p)/\mathrm{K}'_p)$ such that $[R_{\mathrm{K}'_p/\mathrm{K}_p} \phi] = \Phi_N(\bar{\Lambda}_p/\mathrm{K}_p)$.

To prove (*b*) we note that there exists a non-ramified character ϕ of order l in $\Phi(\mathrm{K}'_p)$. As $\mathrm{K}_p/\mathrm{K}'_p$ is totally ramified, $\phi \notin \Phi(\mathrm{K}_p/\mathrm{K}'_p)$, and so $\phi' = R_{\mathrm{K}'_p/\mathrm{K}_p} \phi$ is of order l. Also ϕ' is non-ramified. A non-ramified extension of a field M_p normal over P_p is itself normal over P_p. Thus the fields $(\mathrm{K}'_p)_\phi$ and $(\mathrm{K}_p)_{\phi'}$ are normal, and hence $\phi \in \Phi_N(\bar{\Lambda}(\mathrm{K}'_p)/\mathrm{K}'_p)$, $\phi' \in \Phi_N(\bar{\Lambda}_p/\mathrm{K}_p)$. As the latter group is cyclic of order l, it follows that ϕ' is a generator.

To prove (*a*) one can exclude the trivial case $\mathrm{K}_p = \mathrm{P}_p$; for then $\bar{F}(\Gamma_p, E) = 1$. We thus assume $\mathrm{K}_p = \mathrm{K}'_p \neq \mathrm{P}_p$. Choose ϕ as above in the proof of (*b*). Then $\Gamma((\mathrm{K}_p)_\phi/\mathrm{P}_p)$ is cyclic of l-power order with non-trivial subgroup $\Gamma((\mathrm{K}_p)_\phi/\mathrm{K}_p)$ and non-trivial quotient group

$\Gamma(\mathrm{K}_p/\mathrm{P}_p)$. It follows that the operative class of $(\mathrm{K}_p)_\phi/\mathrm{K}_p/\mathrm{P}_p$ is not the unit class, i.e. $u_p\phi \neq 1$. But as $\mathrm{K}_p/\mathrm{P}_p$ itself is non-ramified, i.e. Γ_p is cyclic, the group $\overline{F}(\Gamma_p, E)$ will be cyclic of order l, and thus will consist of the elements $u_p\phi^r$.

By (12·1) $w_p\phi$ determines $u_p\phi \bmod \overline{F}_N(\Gamma_p, E)$ uniquely, i.e. the mapping

$$w_p\phi \to u_p\phi\,.\,\overline{F}_N(\Gamma_p, E)$$

is defined uniquely, and is a homomorphism, to be denoted by v_p. Then we have:

II. *The sequence of homomorphisms*

$$1 \to w_p\Phi(\mathrm{K}_p/\mathrm{P}_p) \to w_p\Psi(\mathrm{K}_p/\mathrm{P}_p) \xrightarrow{r_p} w_p\Phi(\overline{\Lambda}_p/\mathrm{K}_p) \xrightarrow{v_p} A(\mathrm{K}_p)/\overline{F}_N(\Gamma_p, E) \to 1$$

is exact.

If K_p is non-ramified, then $\mathrm{T}_p = 1$, and so the sequence $1 \to w_p\Psi(\mathrm{K}_p/\mathrm{P}_p) \to w_p\Phi(\overline{\Lambda}_p/\mathrm{P}_p) \xrightarrow{v_p} 1$ is exact, and $\overline{F}(\Gamma_p, E) = A(\mathrm{K}_p)$. Hence:

III. *If* K_p *is non-ramified then for any given character* $\theta_p \in w_p\Phi(\overline{\Lambda}_p/\mathrm{K}_p) = r_p w_p\Psi(\mathrm{K}_p/\mathrm{P}_p)$, *and for any* $\bar{c}_p \in \overline{F}(\Gamma_p, E)$, $\exists \phi \in \Phi(\overline{\Lambda}_p/\mathrm{K}_p)$ *with* $w_p\phi = \theta_p$, $u_p\phi = \bar{c}_p$.

On the other hand, we have:

IV. *If* K_p *is properly ramified, and if*† *for* $p = 2$, $\mathrm{K}_p \supseteq \mathrm{P}_p(\sqrt{2}, \sqrt{-1})$, *then* v_p *is an isomorphism.*

This follows from the fact that $w_p\Phi_{(l)}(\mathrm{P}_p)$ is cyclic when $p \neq 2$, and is the product of two cyclic groups when $p = 2$, while on the other hand, the hypothesis in IV implies the same for $w_p\Phi(\mathrm{K}_p/\mathrm{P}_p)$. Hence $w_p\Psi(\mathrm{K}_p/\mathrm{P}_p) = w_p\Phi(\mathrm{K}_p/\mathrm{P}_p)$. By II this implies that v_p is an isomorphism.

Restating for the sake of completeness in (i) results already contained in theorem 5 we have:

THEOREM 11

(i) *Let for every rational prime* p *non-ramified in* K, λ_p *be a character in* $w_p\Phi_{(l)}(\mathrm{P}_p)$ (*i.e. a rational local residue character at* p *whose* l*th power is the identical character*), *with the proviso that* λ_p *is the identical character for all but a finite number of such primes* p. *Let* $\bar{c}$ *be any element in* $A(\mathrm{K})$. *Then there exists a character* $\phi \in \Phi(\overline{\Lambda}/\mathrm{K})$ *such that*

$$u\phi = \bar{c}, \quad w_p\phi = r_p\lambda_p,$$

for all rational primes p *non-ramified in* K. *In particular for every such prime* p, $u\phi$ *is independent of* $w_p\phi$.

(ii) *Let* p *be a rational prime ramified in* K, *and assume that when* $p = 2$, $\mathrm{P}(\sqrt{2}, \sqrt{-1}) \subseteq \mathrm{K}$. *Then for all* $\phi \in \Phi(\overline{\Lambda}/\mathrm{K})$, $w_p\phi$ *uniquely determines, and is uniquely determined by* $(u\phi)_p \bmod \overline{F}_N(\Gamma_p, E)$. *In particular* $u\phi$ *completely determines* $w_p\phi$. *The correspondence* $w_p\Phi \longleftrightarrow (u\phi)_p\,\overline{F}_N(\Gamma_p, E)$ *is explicitly expressed in the form*: $w_p\phi$ *completely determines, and is completely determined by the set of values*

$$c_p^*(a), \quad c_{p*}(a, b); \tag{12·3}$$

and $w_p\phi = 1$, *if and only if this set of values consists of the element* 1 *only. Here* $\bar{c} = u\phi$. *In* (12·3) b *runs through all idèles* (*or rational numbers*) *and* a *runs through all idèles* (*or rational numbers*) *which are units at* p.

† This assumption will be made throughout in order to avoid lengthy discussion of a special case. The results remain true also if one replaces $\sqrt{2}$, $\sqrt{-1}$ by $\sqrt{2n_1}$, $\sqrt{-n_2}$ where $n_i \equiv 1 \pmod 4$. See also footnote ‡ on p. 418.

Remark. It suffices to take instead of the set of values (12·3) the sets

$$c_p^*(a_p), \quad \text{when} \quad p \equiv 1 \pmod{l}, \tag{12·3a}$$

where a_p is some primitive root mod p,

$$c_l^*(1+l), \quad c_{l*}(1+l, l) \quad \text{when} \quad p = l \neq 2, \tag{12·3b}$$

$$c_2^*(-1), \quad c_2^*(5), \quad c_{2*}(-1, 2), \quad c_{2*}(-1, 5) \quad \text{when} \quad p = l = 2. \tag{12·3c}$$

The significance of theorem 11 is made evident in the following corollary which strengthens the corollary to theorem 5.

Corollary

(i) *For every element* $\bar{c} \in A(\mathrm{K})$, *and for every finite—possibly empty—set* T *of rational primes* p *such that* $p \equiv 1 \pmod{l}$ *or* $p = l$, *and such that* p *is non-ramified in* K, *there exists a character* $\phi \in \Phi(\bar{\Lambda}/\mathrm{K})$, *such that* $u\phi = \bar{c}$, *and such that the relative discriminant of* $\mathrm{K}_\phi/\mathrm{K}$ *is divisible by all primes in* T, *and is co-prime to all rational primes* p *which are non-ramified in* K *and do not lie in* T.

(ii) *Let* p *be a rational prime ramified in* K, *and assume that for* $p = 2$, $\mathrm{P}(\sqrt{2}, \sqrt{-1}) \subseteq \mathrm{K}$. *Let* $\bar{c}$ *be an element of* $A(\mathrm{K})$. *Then* p *is co-prime either to all, or to none of the relative discriminants of the extensions* $\mathrm{K}_\phi/\mathrm{K}$ *with* $\phi \in \Phi(\bar{\Lambda}/\mathrm{K})$, $u\phi = \bar{c}$. *Also* p *is co-prime to all of these relative discriminants if and only if*

(*a*) *when* $p \equiv 1 \pmod{l}$, $c_p^*(a_p) = 1$, *where* a_p *is some* (*arbitrary*) *primitive root* mod p,

(*b*) *when* $p = l \neq 2$, $c_l^*(1+l) = c_{l*}(1+l, l) = 1$,

'*c*) *when* $p = l = 2$, $c_2^*(-1) = c_2^*(5) = c_{2*}(-1, 2) = c_{2*}(-1, 5) = 1$.

Proof of theorem 11. (i) follows by theorems 4 and 5, and by III.

To establish (ii) we observe that T_p is the group of symbols $(\mathrm{K}_p/\mathrm{P}_p;\, a)$, where a runs through the units of P_p. Hence $\bar{c}_p \in \bar{F}_N(\Gamma_p, E)$, if and only if $c_p^*(a) = c_{p*}(a, b) = 1$, for all b, and for all units a. Therefore $\bar{c}_p \bmod \bar{F}_N(\Gamma_p, E)$ is uniquely determined and uniquely determines the set of values $c_p^*(a)$, $c_{p*}(a, b$. (ii) now follows by IV and theorem 4.

The criterion in the remark following the theorem is obtained as follows: Γ_p is generated by the elements $(\mathrm{K}_p/\mathrm{P}_p;\, p)$, and $(\mathrm{K}_p/\mathrm{P}_p;\, a_p)$, where a_p is a primitive root mod p when $p \equiv 1 \pmod{l}$, $a_l = 1+l$ for $p = l \neq 2$, and a_2 takes the values $-1, 5$ for $p = l = 2$. The set of values given in the theorem is then uniquely determined by the elements $c_p^*(a_p)$, $c_{p*}(a_p, p)$, $c_{p*}(a_p, a_p')$, for the stated ranges of a_p, a_p'. The relations in I, however, allow us to omit certain of these values.

Theorem 11 raises some further questions. Thus one can ask whether in turn $u\phi$ is completely determined by $w_p\phi$ for all p ramified in K. This is in fact not true, as will be seen in an example in § 13.

Next the question arises, to what extent the 'full' local character ϕ_p for any prime p is determined by the prescribed characters λ_p in theorem 11 (i), and by $u\phi$. We have seen that the local residue character, i.e. the 'restricted' character $w_p\phi$ was completely determined. Using theorem 11 we can thus reformulate our question: Do $u\phi$ and $w_p\phi$ determine ϕ_p? It is evident that the anwer must be in the negative. For, a determination of ϕ_p implies a criterion for the decomposition of p in K_ϕ, when $w_p\phi = 1$. But such a criterion depends on ϕ, and not solely on the elements $u\phi$ and $w_p\phi$, which for given p do not in general determine ϕ uniquely. By a more detailed analysis a rational prime decomposition law will be derived elsewhere for the fields in $\mathfrak{C}(\mathrm{K}/\mathrm{P})$, when K belongs to a certain special class of fields. Even in this case, however, the law will not depend only on $u\phi$. In the general case no such decomposition criterion in purely rational terms has yet been found.[†]

One can, however, give a more detailed answer to our question. We shall say that a rational prime p is inert in K, if the subgroup $\Phi_N(\mathrm{K}_p/\mathrm{P}_p)$ of non-ramified characters in $\Phi(\mathrm{K}_p/\mathrm{P}_p)$ has order >1. We have

Theorem 12. *Assume that* K *satisfies the hypothesis of theorem* 11, *that if* $2 \mid f$, *then*

$$\mathrm{P}(\sqrt{2}, \sqrt{-1}) \subseteq \mathrm{K}.$$

If p is a rational prime inert in K, *then for all $\phi \in \Phi(\overline{\Lambda}/\mathrm{K})$, $u\phi$ and $w_p\phi$ determine ϕ_p uniquely. If p is a rational prime not inert in* K, *then for every character $\phi \in \Phi(\overline{\Lambda}/\mathrm{K})$, and for every character $\phi'_p \in \Phi(\overline{\Lambda}_p/\mathrm{K}_p)$ such that $w_p\phi = w_p\phi'_p$, there exists a character $\phi' \in \Phi(\overline{\Lambda}/\mathrm{K})$ satisfying $u\phi' = u\phi$, which has ϕ'_p as its p-component.*

Proof. It suffices to prove the theorem when

$$u\phi = 1, \quad w_p\phi = 1. \tag{12·4}$$

Assume first that p is inert. It is required to show that $\phi_p = 1$. By (12·4) $\phi = R\psi$ where one can assume

$$\psi \in \Phi_{(l)}(\mathrm{P}), \quad [\psi] \cap \Phi(\mathrm{K}/\mathrm{P}) = 1. \tag{12·5}$$

It follows that

$$\phi_p = R_p\psi_p, \quad \psi_p \in \Phi_{(l)}(\mathrm{P}_p). \tag{12·6}$$

(12·4) implies $w_p\phi_p = 1$. If now p is non-ramified in K it follows (cf. § 7, proof of (7·6)) that also $w_p\psi_p = 1$. Hence, ψ_p is an element of the group $\Phi_N(\mathrm{P}_p)$ of non-ramified characters in $\Phi(\mathrm{P}_p)$. Hence by (12·6) $\psi_p \in \Phi_N(\mathrm{P}_p) \cap \Phi_{(l)}(\mathrm{P}_p)$. But the group $\Phi_N(\mathrm{P}_p)$ has a unique subgroup of order l and, as p is inert in K, this subgroup is contained in $\Phi(\mathrm{K}_p/\mathrm{P}_p)$. Hence

$$\psi_p \in \Phi(\mathrm{K}_p/\mathrm{P}_p). \tag{12·7}$$

On the other hand, if p is ramified in K then $w_p\Phi_{(l)}(\mathrm{P}_p) \subseteq w_p\Phi(\mathrm{K}_p/\mathrm{P}_p)$, and so

$$\Phi_{(l)}(\mathrm{P}_p) \subseteq \Phi(\mathrm{K}_p/\mathrm{P}_p)\,[\Phi_{(l)}(\mathrm{P}_p) \cap \Phi_N(\mathrm{P}_p)].$$

As p is inert in K, we have again $\Phi_{(l)}(\mathrm{P}_p) \cap \Phi_N(\mathrm{P}_p) \subseteq \Phi(\mathrm{K}_p/\mathrm{P}_p)$ and thus $\Phi_{(l)}(\mathrm{P}_p) \subseteq \Phi(\mathrm{K}_p/\mathrm{P}_p)$. By (12·6) we get again (12·7). But the first equation in (12·6) together with (12·7) implies by theorem 1 that $\phi_p = 1$.

Next assume that p is not inert in K. One has to show that if $\phi'_p \in \Phi_N(\overline{\Lambda}_p/\mathrm{K}_p)$, there exists $\psi \in \Psi(\mathrm{K}/\mathrm{P})$ with $(R\psi)_p = \phi'_p$. One may clearly take $\phi'_p \neq 1$. One can then always find a character ψ with

$$\psi \in \Phi_{(l)}(\mathrm{P}), \quad \psi_p \neq 1, \quad \psi_p \in \Phi_N(\mathrm{P}_p) \tag{12·8}$$

by choosing ψ in such a way that p is inert, but not ramified in the cyclic field P_ψ of degree l. We then have also $\psi_p \in \Phi_{(l)}(\mathrm{P}_p)$, and so $R_p\psi_p \in \Phi_N(\overline{\Lambda}_p/\mathrm{K}_p)$. As, however, p is not inert in K, $\Phi_N(\mathrm{P}_p) \cap \Phi(\mathrm{K}_p/\mathrm{P}_p) = 1$, and so $R_p\psi_p \neq 1$. This character thus generates the cyclic group $\Phi_N(\overline{\Lambda}_p/\mathrm{K}_p)$ of order l. Without loss of generality one may then suppose that

$$R_p\psi_p = \phi'_p. \tag{12·9}$$

But by theorem 4 we then have $(R\psi)_p = \phi'_p$.

[†] It was in fact the aim here to show that the set $\mathfrak{C}(\mathrm{K}/\mathrm{P})$ could be determined rationally without the use of a decomposition law.

13. An example

This concluding section is to illustrate the results obtained. The example to be considered is the class of fields K, such that (i) $\Phi(\mathrm{K}/\mathrm{P})$ is the direct product of two groups of order l, (ii) the conductor f is divisible by precisely two rational primes p_1, p_2 with $p_1 \equiv p_2 \equiv 1 \pmod{l}$. This is the simplest representative class of fields available. The cyclic fields K would not do for the purpose. For when K is cyclic, then all fields in $\mathfrak{C}(\mathrm{K}/\mathrm{P})$ are absolutely Abelian, and can therefore be dealt with by classical methods.

Let then K be a field satisfying the conditions (i), (ii) above. If for $i = 1, 2$, χ_i is a primitive lth power residue character mod p_i then $w^{-1}\chi$, $w^{-1}\chi_2$ is a basis of $\Phi(\mathrm{K}/\mathrm{P})$, and the elements γ_1, γ_2 of Γ satisfying $[w^{-1}\chi_i](\gamma_j) = \mathrm{e}(\delta_{ij}/l)$ form a basis of Γ. Every element $\bar{c}$ of $\bar{F}(\Gamma, E)$ is uniquely determined by, and uniquely determines the invariants $C^*(\gamma_1)$, $C^*(\gamma_2)$, $C_*(\gamma_1, \gamma_2)$ mod l, and for every given sequence of three integers mod l there exists an element $\bar{c}$ of $\bar{F}(\Gamma, E)$ having these as invariants. The group $\bar{F}(\Gamma, E)$ is thus the direct product of three groups of order l. A necessary and sufficient condition for $\bar{c}$ to lie in $A(\mathrm{K})$ is that

$$\left.\begin{aligned} \chi_2(p_1)^{-C_*(\gamma_1, \gamma_2)} &= \mathrm{e}\,(1/l^2)^{(p_1-1)\,C^*(\gamma_1)}, \\ \chi_1(p_2)^{C_*(\gamma_1, \gamma_2)} &= \mathrm{e}\,(1/l^2)^{(p_2-1)\,C^*(\gamma_2)}. \end{aligned}\right\} \qquad (13\cdot1)$$

We see here clearly exhibited the property of the left-hand side to depend on the mutual congruence behaviour of p_1 and p_2, and the right-hand side to depend on the congruence behaviour of p_1, p_2 mod l. In what follows the several cases that may arise accordingly will be dealt with. This information is presented in table 1.

Table 1

1	2	3	4
$p_1 \equiv p_2 \equiv 1 \pmod{l^2}$ $\chi_1(p_2) = \chi_2(p_1) = 1$	$A(\mathrm{K}) = \bar{F}(\Gamma, E)$ —	$[l, l, l]$, $[l^2, l]$ B, C	$[2, 2, 2]$, $[4, 2]$ D, Q
$p_1 \equiv p_2 \equiv 1 \pmod{l^2}$ $\chi_1(p_2) \neq 1$	$C_*(\gamma_1, \gamma_2) \equiv 0$ —	$[l, l, l]$ $[l^2, l]$	$[2, 2, 2]$ $[4, 2]$
$p_2 \not\equiv p_1 \equiv 1 \pmod{l^2}$ $\chi_1(p_2) = \chi_2(p_1) = 1$	$C^*(\gamma_2) \equiv 0$ —	$[l, l, l]$, $[l^2, l]$ B, C	$[2, 2, 2]$, $[4, 2]$ D
$p_2 \not\equiv p_1 \equiv 1 \pmod{l^2}$ $\chi_1(p_2) \neq 1$, $\chi_2(p_1) = 1$	$C_*(\gamma_1, \gamma_2) - \frac{p_2-1}{l} C^*(\gamma_2) \equiv 0$ —	$[l, l, l]$, $[l^2, l]$ C	— —
$p_2 \not\equiv p_1 \equiv 1 \pmod{l^2}$ $\chi_2(p_1) \neq 1$, $\chi_1(p_2) \neq 1$	$C_*(\gamma_1, \gamma_2) \equiv 0$ $C^*(\gamma_2) \equiv 0$	$[l, l, l]$ $[l^2, l]$	$[2, 2, 2]$ $[4, 2]$
$p_1 \not\equiv 1$, $p_2 \not\equiv 1 \pmod{l^2}$ $\chi_1(p_2) = \chi_2(p_1) = 1$	$C^*(\gamma_1) \equiv 0$ $C^*(\gamma_2) \equiv 0$	$[l, l, l]$ B	— —
$p_1 \not\equiv 1$, $p_2 \not\equiv 1 \pmod{l^2}$ $\chi_1(p_2) \neq 1$, $\chi_2(p_1) \neq 1$	$C_*(\gamma_1, \gamma_2) + \frac{p_1-1}{l} C^*(\gamma_1) \equiv 0$ $C_*(\gamma_1, \gamma_2) - \frac{p_2-1}{l} C^*(\gamma_2) \equiv 0$	$[l, l, l]$ C	— —
$p_1 \not\equiv 1$, $p_2 \not\equiv 1 \pmod{l^2}$ $\chi_2(p_1) \neq 1$, $\chi_1(p_2) = 1$	$C_*(\gamma_1, \gamma_2) + \frac{p_1-1}{l} C^*(\gamma_1) \equiv 0$ $C^*(\gamma_2) \equiv 0$	$[l, l, l]$ C	$[2, 2, 2]$ D

In table 1 each row refers to a particular case, which is determined by the entry in the first column, stating the congruence relations assumed for p_1 and p_2. Any case not dealt with in the table can be derived from a given one by permuting the indices. For $l = 2$, some of the stated cases can in fact not occur as they contradict the quadratic reciprocity law. The second column determines the group $A(\mathrm{K})$ in each case. This is done mainly by congruence conditions mod l imposed on the invariants. The particular choice of the characters χ_1, χ_2 is still free for $l \neq 2$; we can thus assume without loss of generality

$$\left.\begin{aligned} \chi_1(p_2) &= 1, \quad \text{or} \quad \chi_1(p_2) = \mathrm{e}(1/l), \\ \chi_2(p_1) &= 1, \quad \text{or} \quad \chi_2(p_1) = \mathrm{e}(1/l). \end{aligned}\right\} \tag{13·2}$$

For $l = 2$, (13·2) will hold in any case.

Also given in each case are the abstract groups of order l^3 which are realized in the form $\Gamma(\Lambda/\mathrm{P})$ for some $\Lambda \in \mathfrak{C}(\mathrm{K}/\mathrm{P})$. This information is embodied in the third column for $l \neq 2$, and in the last column for $l = 2$; when $l = 2$ the entry in the 'impossible' cases is omitted. The Abelian groups of order l^3 will simply be denoted by their invariants. As Γ is non-cyclic $[l^3]$ cannot occur, but $[l^2, l]$ and $[l, l, l]$ will occur. For $l = 2$, denote the dihedral group of order 8 by D, and the quaternion group of Q. If $l \neq 2$, denote by B the non-Abelian group of order l^3 and exponent l, and by C the non-Abelian group of order l^3 and exponent l^2.

We observe that for fields K of the type considered here the mapping u^* is an isomorphism (corollary, theorem 5). Thus for every $\bar{c} \in A(\mathrm{K})$ there exists a unique character $\phi_{\bar{c}} \in \Phi(\overline{\Lambda}/\mathrm{K})$ with the following properties (denoting by K_i the invariant field of γ_i):

(1) $\phi_{\bar{c}}(\mathfrak{A}) = 1$ for every unit idèle $\mathfrak{A}$, which has components 1 at all infinite prime divisors, and all prime divisors lying above p_1 and p_2.

(2) If $N_{\mathrm{K}/\mathrm{K}_i}\mathfrak{A} = \mathfrak{a}^l$, $(\mathrm{K}/\mathrm{K}_i;\, \mathfrak{a}) = \gamma_i$, then

$$\phi_{\bar{c}}(\mathfrak{A}) = \mathrm{e}\,(C^*(\gamma_i)/l).$$

(3) If $N_{\mathrm{K}/\mathrm{K}_2}\mathfrak{A} = \gamma_1\mathfrak{a}.\mathfrak{a}^{-1}.\alpha$, $(\mathrm{K}/\mathrm{K}_2;\, \mathfrak{a}) = \gamma_2$, $\alpha \in V_{\mathrm{K}_2}$, then

$$\phi_{\bar{c}}(\mathfrak{A}) = \mathrm{e}\,(C_*(\gamma_1, \gamma_2)/l).$$

Also $u\phi_{\bar{c}} = \bar{c}$. $\phi_{\bar{c}_1}.\phi_{\bar{c}_2} = \phi_{\bar{c}_1.\bar{c}_2}$.

Every character $\phi \in \Phi(\overline{\Lambda}/\mathrm{K})$ has then a unique representation of the form

$$\phi = \phi_{\bar{c}}.R\psi, \tag{13·3}$$

where ψ runs through all rational idèle class characters satisfying $\psi(\mathfrak{a}^l) = 1$, for all rational idèles $\mathfrak{a}$, $\psi(\mathfrak{a}) = 1$, if $\mathfrak{a}$ is a rational unit idèle with components 1 at p_1, p_2 and at the infinite prime divisor. The character $R\psi$ is defined by

$$R\psi(\mathfrak{A}) = \psi(N_{\mathrm{K}/\mathrm{P}}\mathfrak{A}).$$

If ϕ is given by (13·3), and $\mathfrak{p}$ is a finite prime divisor in K, lying above the rational prime divisor p, and if $U_{\mathfrak{p}}$ is the group of idèles in K which are units at $\mathfrak{p}$ and have component 1 elsewhere, then

$$\phi(\mathfrak{A}) = 1, \quad \text{for all } \mathfrak{A} \in U_{\mathfrak{p}}$$

if and only if

(i) when $p \neq p_1, p_2$, $\psi(\mathfrak{a}) = 1$ for all rational idèles $\mathfrak{a}$ which are units at p and have component 1 elsewhere;

(ii) when $p = p_i$, $C^*(\gamma_i) \equiv 0 \pmod{l}$.

In particular, if $\bar{c}$ has invariants $C_*(\gamma_1, \gamma_2) = 1$, $C^*(\gamma_i) = 0$ for $i = 1, 2$, then $\phi_{\bar{c}}$ is non-ramified. Thus in the case when $\chi_1(p_2) = \chi_2(p_1) = 1$, $\Phi(\overline{\Lambda}/\mathrm{K})$ contains a character ϕ with $u\phi \neq 1$, $w_p \phi = 1$, for all p. This is the required counter example, showing that the local residue characters $w_p \phi$, for all p, do not determine $u\phi$ uniquely.

References

Brauer, R. 1947 *Ann. Math. Princeton*, (2), **48**, 79.

Chevalley, C. 1940 *Ann. Math. Princeton*, (2), **41**, 394.

Chevalley, C. 1954 *Class field theory*. Nagoya University.

Fröhlich, A. 1954 *Proc. Lond. Math. Soc.* (3), **4**, 235.

Hasse, H. 1947 *Abh. dtsch. Akad. Wiss. Berl. Kl. Math. Nat.* **8**, 1.

Hasse, H. 1948 *Math. Nachr.* **1**, 40.

Hochschild, G. & Nakayama, T. 1952 *Ann. Math. Princeton*, (2), **55**, 348.

Jehne, W. 1952 *Abh. math. Sem. Hamburg Univ.* **18**, 70.

Nakayama, T. 1952 *Ann. Math. Princeton*, (2), **55**, 73.

Reichardt, H. 1936 *Math. Z.* **41**, 218.

Reichardt, H. 1937 *J. Reine Angew. Math.* **177**, 1.

Šafarevič, I. R. 1954*a* *Izv. Akad. Nauk SSSR*, **18**, 216 (*Amer. Math. Soc. Transl.* (2), **4**, 107).

Šafarevič, I. R. 1954*b* *Izv. Akad. Nauk SSSR*, **18**, 389 (*Amer. Math. Soc. Transl.* (2), **4**, 151).

Šafarevič, I. R. 1954*c* *Izv. Akad. Nauk SSSR*, **18**, 525 (*Amer. Math. Soc. Transl.* (2), **4**, 185).

Scholz, A. 1929 *Math. Z.* **30**, 332.

Scholz, A. 1936 *Math. Z.* **42**, 161.

Weil, A. 1951 *J. Math. Soc. Japan*, **3**, 1.

Wolf, P. 1953*a* *Math. Nachr.* **9**, 281.

Wolf, P. 1953*b* *Math. Nachr.* **10**, 233.

Wolf, P. 1956 *Math. Forschungsberichte* III.