Sugaku Expositions
Volume 8, Number 1, June 1995

A FOUNDATION OF CLASS FIELD THEORY APPLYING PROPERTIES OF SPATIAL FIGURES

TOMIO KUBOTA

This article is prepared as notes of the general address given by the author at the 1991 Annual Meeting of the Mathematical Society of Japan held at Keio Gijuku University and also is an expository explanation of the author's paper *Geometry of numbers and class field theory*, Japanese J. Math. **13** (1987), 235–275.

1. The main point of class field theory

We begin with a brief explanation of class field theory. Class field theory is concentrated in an assertion called Artin's reciprocity law. There are various forms of Artin's reciprocity law, but we use here the shortest form.

Denote by F an algebraic number field of finite degree, by K an abelian extension of F of finite degree, by $G(K/F)$ the Galois group of K/F, and furthermore by $\mathfrak{o}_K$, $\mathfrak{o}_F$ the rings of integers of K, F respectively. Then, for every prime ideal $\mathfrak{p}$ of F (of $\mathfrak{o}_F$), there exists an element $\sigma = (\frac{K/F}{\mathfrak{p}})$, called the Frobenius automorphism of $G(K/F)$. It is defined by the condition $\alpha^\sigma \equiv \alpha^{N\mathfrak{p}}$ $(\operatorname{mod} \mathfrak{p})$, $N\mathfrak{p}$ being the norm $(\mathfrak{o}_F : \mathfrak{p})$ of $\mathfrak{p}$. The Frobenius automorphism is determined uniquely except for a finite number of special prime ideals. Take next an arbitrary integral ideal $\mathfrak{a}$ of F with the decomposition $\mathfrak{a} = \mathfrak{p}_1\mathfrak{p}_2\cdots\mathfrak{p}_r$ into prime factors. The factors may contain the same ideals. Then $(\frac{K/F}{\mathfrak{a}}) = (\frac{K/F}{\mathfrak{p}_1})\cdots(\frac{K/F}{\mathfrak{p}_r})$ is an element of $G(K/F)$, called the Artin symbol of $\mathfrak{a}$, which is determined uniquely unless $\mathfrak{a}$ is divisible by a finite number of special prime ideals.

Assertion A (Artin's reciprocity law). There exists an ideal $\mathfrak{m}$ of F determined by K/F such that $(\frac{K/F}{(\alpha)}) = 1$ holds for the principal ideal (α) generated by an integer α of F, whenever α satisfies the congruence $\alpha \equiv 1 \pmod{\mathfrak{m}}$ and is totally positive, i.e., the image of α by every embedding of F into $\mathbf{R}$ is positive.

This assertion shows the most essential part of Artin's reciprocity law. Namely, if α is screened by a congruence condition and a sign condition, then the Artin symbol of (α) is 1 (if no embedding of F into $\mathbf{R}$ exists, then every

This article originally appeared in Japanese in Sūgaku **44** (1) (1992), 1–12.

1991 *Mathematics Subject Classification*. Primary 11A15, 11B50.

$\alpha \neq 0$ is totally positive, so the sign condition falls off). Once this assertion has been verified, all theorems of class field theory can be deduced smoothly and straightforwardly. Thus we may say that class field theory is concentrated in Assertion A.

2. Artin's reciprocity law for special extensions

Let us consider Artin's reciprocity law where K/F is a special extension. If K/F is a cyclotomic extension, i.e., is obtained by adjoining a root of unity, then Artin's reciprocity law becomes a very simple fact and, as is found in many textbooks of number theory, can be proved easily and directly.

Next, we consider another typical abelian extension called a Kummer extension, which is of the form $K = F(\sqrt[n]{\alpha})$ provided that F contains the group μ_n of the nth roots of unity. It may be assumed that α is an integer, $\alpha \in \mathfrak{o}_F$, and K/F is a cyclic extension. In this case the Artin symbol is related to the symbol $(\frac{\alpha}{\beta})_n$, called the power residue symbol, through the equality

$$\sqrt[n]{\alpha}^{\sigma} = \left(\frac{\alpha}{\beta}\right)_n \sqrt[n]{\alpha}, \qquad \sigma = \left(\frac{K/F}{(\beta)}\right).$$

Since the Artin symbol $(\frac{K/F}{(\beta)})$ is an element of the Galois group $G(K/F)$, it maps $\sqrt[n]{\alpha}$ onto an element of K that differs from $\sqrt[n]{\alpha}$ only by a factor in μ_n. The factor turns out to be the power residue symbol $(\frac{\alpha}{\beta})_n$ of $\alpha \bmod \beta$. Artin's reciprocity law is, therefore, expressed in the following different form:

Assertion K (The reciprocity law of the power residue symbol). There exists an ideal $\mathfrak{m}(\alpha)$ of F, determined by $\alpha \in \mathfrak{o}_F$, such that $(\alpha/\beta)_n = 1$ holds whenever $\beta \in \mathfrak{o}_F$ satisfies the congruence $\beta \equiv 1 \pmod{\mathfrak{m}(\alpha)}$ and is totally positive.

The symbol $(\alpha/\beta)_n$ in this assertion is the power residue symbol $(\frac{\alpha}{\beta})_n$. Throughout the sequel, power residue symbols will always be written as $(\alpha/\beta)_n$.

Assertion K is a special case of Artin's reciprocity law restricted to the Kummer extension. But, unlike the case restricted to a cyclotomic field, it cannot be proved easily. Until the present time, the special case of the reciprocity law for the Kummer extension could be deduced only by means of all results, or practically all essential arguments, of class field theory.

By the way, the reciprocity law of the power residue symbol in the form of Assertion K is "asymmetric". In fact, the reciprocity law of the power residue symbol is often written as an equality roughly between $(\alpha/\beta)_n$ and $(\beta/\alpha)_n$. If such a form is called "symmetric", the above assertion that the value of the symbol becomes 1 under a sufficiently strong screening of β should be called asymmetric, since the latter contains no symmetry. But, there is no essential difference between the two.

If the basic field F is the rational number field $\mathbf{Q}$, and $n = 2$, then the power residue symbol is the classic quadratic residue symbol $(\frac{a}{b})$. The quadratic residue symbol has a direct definition. For instance, if $b = p$ is an odd prime, it is defined by $(\frac{a}{p}) \equiv a^{(p-1)/2} \pmod{p}$, $(\frac{a}{p}) = \pm 1$, for $a \in \mathbf{Z}$ which is prime to p. The power residue symbol $(\alpha/\beta)_n$ in the general case can be defined directly and similarly. The above equality containing both the Artin symbol and the power residue symbol is fundamental but is not a definition of the power residue symbol.

3. Questions on the construction of class field theory

As was already described, Artin's reciprocity law is simple, clear, and beautiful both in its original form and in the specialization to the power residue symbol. But, if one reads its proof—which amounts to learning the whole class field theory—various questions arise. Let us discuss some of these questionable points.

1. **On the structure of the theory.** Every abelian extension is obtained as a subfield of a cyclotomic extension followed by a Kummer extension. The reciprocity law for a cyclotomic extension is, as mentioned in §2, easily proved. Therefore, a straightforward proof of the general reciprocity would be obtained if one could prove the reciprocity of the Kummer extension by some method based on the special situation and then use both special results together to get the general case. Why, instead of such a plain way, the general case must first be constructed in order to obtain a Kummer case is also mentioned in §2.

2. **On the methodology.** Also, as mentioned in §2, the notion of the power residue symbol $(\alpha/\beta)_n$ is constructed within the basic field F, and so its reciprocity is also an assertion concerning solely the field F. Why, however, does its proof require the structure of extension fields including very precise behaviors of ideal groups, unit groups, etc., under the operation of the Galois group?

3. **On the classical theory of quadratic residue symbols.** The quadratic residues of rational integers have historically been treated in various ways. Some are elementary, and some apply figures. But, their theoretical meanings are not all made clear by class field theory.

4. **Gauss sums and Jacobi sums.** It was Eisenstein who first published the proof of the reciprocity laws of the cubic and biquadratic power residue symbols in $\mathbf{Q}(\sqrt{-3})$ and $\mathbf{Q}(\sqrt{-1})$, respectively. In his proof, he used the so-called Gauss sums and Jacobi sums. These sums are very interesting quantities in number theory and have many applications. But in class field theory, they have disappeared.

5. **On Gauss's theory of biquadratic residues.** After having proved the quadratic reciprocity law in the rational number field, Gauss first tried in vain to build up the theory of biquadratic residues within the rational number field. But he finally found, to his great pleasure, that the biquadratic reciprocity law holds completely in the same form as the quadratic reciprocity law in $\mathbf{Q}$ whenever Gauss's integers $a+bi$ $(a, b \in \mathbf{Z})$ are introduced. This fact is the first discovery of the principle that the nth power residues can be treated smoothly only when

the basic field contains the nth roots of unity, as is quite common knowledge at present. But in class field theory, it is no longer an important condition whether or not the basic field contains the nth roots of unity. Why is this so?

6. Complex multiplication. The reason why Artin's reciprocity law for the cyclotomic extension is easy to get is that the extension is obtained concretely by the values of the exponential function. If a good function is found, which in a similar way generates general abelian extensions, then Artin's reciprocity law in the general case should have a nice proof. In fact, such a situation is realized by means of elliptic functions when the basic field is imaginary quadratic. But the path in this direction is too hard to trace up to the goal and class field theory does not shed any light there.

7. On automorphic functions. Hecke showed that the quadratic reciprocity law in an arbitrary number field is a consequence of the transformation formula of a theta function. Although a partly related fact can already be found in Gauss's work, it is very remarkable that the quadratic reciprocity law in the general case can be proved without any connection with field extensions. Why should an automorphic function like a theta function appear in the investigation of the power residue, while no automorphic function appears in class field theory?

4. CHANGE OF VIEW POINT

Through various opportunities, the author learned that the questions discussed in §3 had also been asked by some other mathematicians, although not completely in the same form. A common opinion of those mathematicians seemed to be that an important fact in number theory is still hidden and, after a splendid discovery, all questions will be answered correctly to erase all discontent. This is certainly a reasonable comment. The author, too, believed this and endeavored for a rather long time to find a hidden truth, mainly in the analytic direction, concerning automorphic functions as well as special functions. But, the conclusion that the author finally attained was totally unexpected, namely, that Assertion K, stated as the reciprocity law of the power residue symbol in §2, was a plain fact. More precisely, the reciprocity law of the power residue symbol merely says that the lattice points in a space are arranged under a certain special rule, and Assertion K is, perhaps with some exaggeration, evident almost at a glance as soon as lattice points and other figures in a space are observed from a slightly new angle that has not been noticed before. Accordingly, Assertion K is proved without any help of Kummer extensions. Of course, there remains the question: why do the power residues have connections with Kummer extensions, complex multiplication, automorphic functions, etc.? A short answer to this question would be that a fundamental fact can support many things. Many relationships—for instance, one between automorphic functions and the reciprocity law—can furnish sources of new research. Such research possibly yields as a by-product a new proof of the reciprocity itself. But, at any rate, a proof of a simple assertion based upon incomparably deep facts would not be of utmost importance. In the following sections, we shall explain how the reciprocity law of the power residue symbol can be seen as evident at a glance.

5. Cyclotomic crystallographic group

We denote by F an algebraic number field of finite degree, assume $F \supset \mu_n$ (the group of the nth roots of unity), put $F \otimes_{\mathbf{Q}} \mathbf{R} = V$ $(\cong \mathbf{R}^N)$, and regard V as a topological vector space, that is, V is a linear space without metric, and n is an arbitrary natural number. The space V is also the infinite component of the adèle ring of F, and N is the absolute degree of F. The mapping $z \to \zeta z$, $(\zeta \in \mu_n,\ z \in V)$, which is (so to speak) the rotation by ζ, operates on V as well as the translation $z \to z + a$ $(a \in \mathfrak{o}_F)$, by an integer a. The group Γ generated by these two kinds of linear transformations will be called the cyclotomic crystallographic group. In general a crystallographic group is a transformation group of a vector space whose fundamental domain is a polyhedron. This is in fact the case for our group Γ. Furthermore, as an important fact in our investigation, a fundamental domain of Γ is given by parallelotopes. Here, a parallelotope means a direct product of segments as a set and is a higher-dimensional generalization of a parallelogram. But, in general, it is not possible to obtain a fundamental domain of Γ by a single parallelotope; a finite number of parallelotopes are needed.

From now on, until the end of the present article, every figure will be drawn as if $F = \mathbf{Q}(\sqrt{-3})$. In this case, we may understand that $V = \mathbf{C}$. But, everything we state in the sequel is valid in the general case. First we explain how to construct a fundamental domain of Γ as a parallelotope. In Figure 1 (see p. 6), the dotted lines show a fundamental domain of the group consisting of only translations by integers, i.e., a period parallelogram used in the theory of elliptic functions. This parallelogram is not clearly divided into three parallelotopes which are mapped on each other under the operation of the roots of unity. So we proceed in a different way and consider a right hexagon surrounded by six right middle lines of 0 and six nearest integers. This hexagon is divided into three parallelograms each of which forms a fundamental domain of the finite group of rotations induced by the roots of unity acting on the hexagon. Thus we get a fundamental domain $P = \Gamma \backslash V$. This technique works in the general case. The fundamental domain P together with the so-called Gauss's lemma gives a link between the power residue symbol and figures. Take an arbitrary $t \in P$, and let $(\alpha/\beta)_n$ be the power residue symbol in our investigation. Then, since P is a fundamental domain of the cyclotomic crystallographic group Γ, αt can be mapped by Γ on a point $t' \in P$. In other words, αt is equal to the point obtained from t' first by multiplying by an element $\varepsilon(\alpha, t)$ of μ_n and then operating a translation given by the elements of $\mathfrak{o}_F$. Therefore, we may write $\alpha t \equiv \varepsilon(\alpha, t)t' \pmod 1$. Using now a terminology in the theory of abelian varieties, call an element of $\beta^{-1}\mathfrak{o}_F$ a β-division point. Then, the point t' corresponding to a β-division point t is again a β-division point and

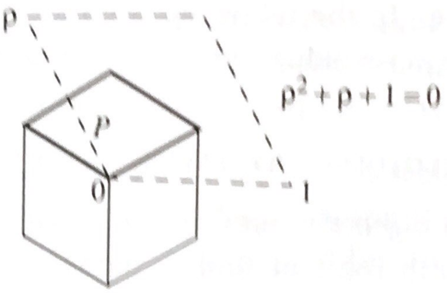

FIGURE 1

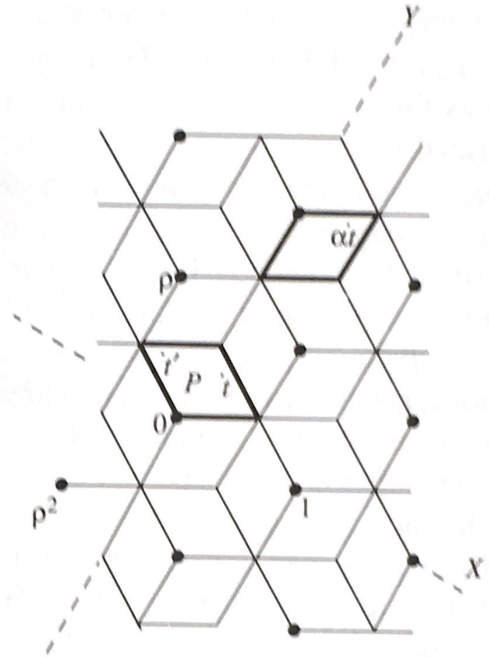

FIGURE 2. CRYSTAL STRUCTURE

Gauss's Lemma holds in the following form:

Gauss's Lemma. $(\alpha/\beta)_n = \prod_t \varepsilon(\alpha, t)$. *(The product ranges over β-division points ($\neq 0$) in P.)*

We call $\varepsilon(\alpha, t)$ the sign of $t \in P$. Every β-division point has a sign that is uniquely determined, and their product is equal to $(\alpha/\beta)_n$. Figure 2 is prepared in order to explain the meaning of the sign more intuitively. The black dots represent integers, and the fundamental domain P is mapped by an element of Γ onto a parallelogram whose one vertex is an integer so that the whole plane is divided according to a certain crystal structure. The images of P face in general in different directions from the original P, and the difference is caused by rotations by roots of unity. In particular, the sign $\varepsilon(\alpha, t)$ of t is that root of unity that shows how much the parallelogram containing αt is rotated in comparison with the original P.

For each β-division point t ($\neq 0$) in P, the sign $\varepsilon(\alpha, t)$ is determined and it is one of the finite elements of μ_n. Therefore, if it is verified that the number of t with one and the same $\varepsilon(\alpha, t)$ is a multiple of n, then $(\alpha/\beta)_n$ becomes evident.

6. Deformation of parallelotopes

Unfortunately, the good situation, as mentioned at the end of the preceding section, does not appear as long as a naive fundamental domain like the parallelotope P in Figures 1 and 2 is being used. But, there are many possibilities to make up fundamental domains. So, we try somehow to deform P to obtain a good distribution of β-division points.

For the sake of simplicity, we consider for a moment a double period group operating on a plane and assume that its period parallelogram is the figure on the left-hand side of Figure 3. If the figure is deformed into the domain assigned with I on the right-hand side of Figure 3, the result is a domain with one part convex and the other corresponding part concave. Then, the new figure is still a fundamental domain. Or, if one side of the original parallelogram is replaced by a zigzag line as II on the right-hand side of Figure 3, then there still remains a fundamental domain. In this case, it should be noted that a minor parallelogram in II that looks reversed should be regarded as a negative domain. Furthermore, as in III on the right-hand side of Figure 3, a fundamental domain can also be constructed by replacing two sides of the original parallelogram by zigzag lines. In general, a parallelogram is spanned by two segments (vectors) starting from a common point. Namely, the parallelogram is the totality of the sums of two points each taken from one of the two sides. In this sense, a parallelogram is considered as a direct sum of two segments. In the same sense, the figures in I, II, and III on the right-hand side of Figure 3 can be considered to be direct sums of two curves or zigzag lines obtained by deforming the two sides of the original parallelogram. What we are going to do is to deform a fundamental domain P, given as a sum of parallelotopes, of the cyclotomic crystallographic group acting on the vector space V into a sum of minor parallelotopes with $+$ and $-$ signs just as two cases II and III of Figure 3 are mixed. To do this, we first replace all those sides of P with zigzag lines that span P, that is, that start from the origin of V, and then take their direct sums.

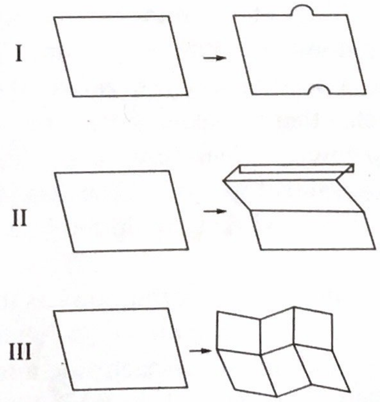

FIGURE 3. DEFORMATION OF PARALLELOTOPES

To perform such a deformation nicely, the whole process should be divided into two steps. Assuming that $(\alpha/\beta)_n$ is the power residue symbol in question, the first deformation is in connection with α. The straight segment in I of Figure 4 stands for a side of P starting from the left end, which is the origin of V. This segment is deformed into a zigzag line, as shown in II of Figure 4, whose vertices are all α-division points. Namely, the zigzag line turns only at an α-division point. Here, α-division points should not be passed arbitrarily. The original segment is first deformed into a rather rough zigzag line as shown by the dotted lines in I of Figure 4, and then each side of the rough zigzag line is refined in accordance with the decomposition $1 = \frac{1}{3}(1-\rho+1-\rho^2)$, $(\rho^2+\rho+1=0)$, of 1, if the situation is as special as drawn there. In the general case, too, the deformation is performed in a similar way based on a simple number-theoretical identity. After this first step concerning α, the resulting zigzag line is smooth in a certain sense and passes α-division points which are its vertices, while the starting point and the end point are unchanged. Next, we turn to the deformation with respect to β. To do this, we put $\beta = 1+\beta_0$ and multiply the zigzag line in II of Figure 4 by β_0/β. Since β is screened by the condition to be congruent to 1 modulo a sufficiently large integer, β_0 is divisible by a sufficiently large integer. On the other hand, β_0/β may be assumed to be sufficiently close to 1, because β may be multiplied by an nth power of an integer. Therefore, the figure after the multiplication by β_0/β is not much different from the original, but it cannot fill the room between the original starting point and the end point. To fill the remaining small rooms, we consider a vector which is obtained from the straight segment in I of Figure 4 by multiplying by $1/(2\beta)$ and joining two copies of the vector to the above figure both at the starting point and at the end. This completes the deformation with respect to β. Taking the direct sum of the sides starting from 0 of P, all after having been deformed into the form as III of Figure 4, we get the desired fundamental domain. The domain, in its most simplified form, is shown on the left-hand side of Figure 5. Dotted lines indicate the original parallelotope, and its sides starting from the origin 0 of the vector space V after the deformation are two thick zigzag lines. Most of the minor parallelotopes are positive, but reversed ones are negative domains. Besides, a minor parallelotope indicated by dotted lines means that a positive and a negative parallelotope occur at the same time and cancel each other. Furthermore, the whole figure itself does not have any particular symmetry. Therefore, it is a coincidence that a dotted line showing the original parallelotope looks like passing a vertex of a minor parallelotope, and it is quite natural that the dotted lines and parallelotopes are in irregular position.

Such a fundamental domain after a deformation has the property that, roughly speaking, every minor parallelotope contains β-division points with a common sign which line up in the direction of each side and are placed in number equal to multiples of n. Thus, $(\alpha/\beta)_n = 1$ is obvious, and the reciprocity law of the power residue symbol in the form of Assertion K is proved.

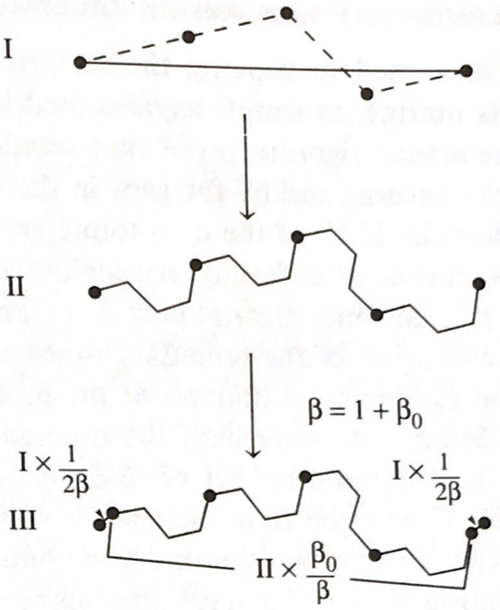
I
II
$\beta = 1 + \beta_0$
$\mathrm{I} \times \frac{1}{2\beta}$
$\mathrm{I} \times \frac{1}{2\beta}$
III
$\mathrm{II} \times \frac{\beta_0}{\beta}$

FIGURE 4

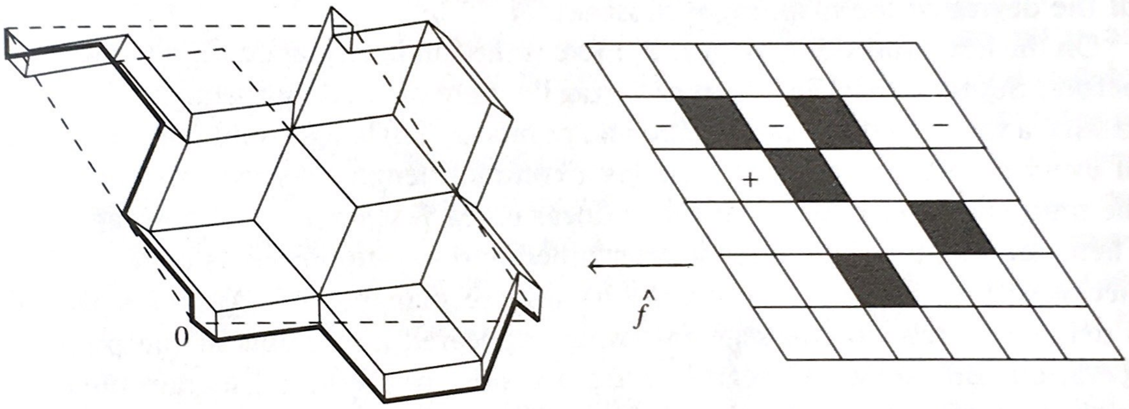

FIGURE 5

This completes the explanation of the most important fundamental principle contained in the present article. Looking back, we will see that no difficult notion is needed for the purpose of proving the reciprocity law of the power residue symbol—no extension field at all. The structure theory of algebraic number fields is not necessary either. Most basic theorems in the structure theory of algebraic number fields such as Dirichlet's unit theorem or the finiteness of the class number are unnecessary, and units play no role at all. Moreover, even ideals need not be really used, since the power residue symbol itself is defined directly by means of Gauss's Lemma concerning only integers. What we really need are only naive and intuitional properties of lattice points and other figures in a space, and all notions used in the arguments are only those that already existed at the time of Euler. A regrettable difficulty is that the usual contemporary mathematical notation makes unclear and strange the figures and manipulations that are too elementary and primitive. The greatest concern to be addressed now is to develop suitable notation so that easy concepts may be expressed simply.

7. Supplementary remarks on crucial points

Whereas the main idea used in proving the reciprocity law of the power residue symbol is, in its outline, as simple as described in §6, there are several important details in the actual, rigorous proof that should be treated carefully. Let us here discuss such concerns and fill the gaps in the preceding description.

1. If a fundamental domain $\Gamma\backslash V$ of the cyclotomic crystallographic group Γ has been constructed by means of deformed parallelotopes as in Figure 5, etc., the reciprocity law $(\alpha/\beta)_n$ becomes clear almost at a glance as explained in §6. Here, however, the investigation of the boundary is somewhat incomplete. As far as the volume of the fundamental domain or the integration of a function over the fundamental domain is concerned, the boundary is not substantial. But, for our purposes, a representative set of β-division points that are not mapped to each other by Γ must be given rigorously, so it must be made clear which point should be taken when two points on the boundary are mapped to each other by the operation of Γ. To settle this point satisfactorily, we use elementary ideas in classical combinatorial topology. Among others, the notion of the degree of the mapping is most useful.

On the left-hand side of Figure 5, there is the fundamental domain mentioned before. Suppose that the two thick zigzag lines are pressed into straight segments in such a way that their starting and end points are unchanged and that the image of every segment in a zigzag line has a common length. Assume furthermore, the mapping determined as above is linear on each segment in the zigzag lines. Then, the mapping is uniquely determined and one-to-one; it is a PL-map (a piecewise linear map). We denote its inverse map by $\hat{f}$. At this stage, $\hat{f}$ is defined merely on two segments which appeared as a result of the pressing operation. But, these two segments are two sides of the parallelogram building up the domain on the right-hand side of Figure 5, one at the bottom and the other on the left, while the sums of two points each taken from one of the two segments form the parallelogram. Hence, $\hat{f}$ is additively extended to a PL-map from one domain to another and is also extended to a PL-map from the space V to itself, because both domains are fundamental domains of the cyclotomic crystallographic group. But, $\hat{f}$ is not one-to-one. On the right-hand side of Figure 5, $\hat{f}$ degenerates on a shadowed minor parallelotope, and its image is constant along a direction in the shadow. Incidentally, a parallelotope marked with $-$ in the same figure shows that its image by $\hat{f}$ is reversed. The image of $\hat{f}$ of a parallelotope without sign is a positive domain. A minor parallelotope that is exceptionally marked with $+$ shows that its image is cancelled by the image of the minor parallelotope marked with $-$, which lies right-upward of the former one. The situation of the degeneration of $\hat{f}$ on a minor parallelotope can be described easily by using simple number-theoretical data. Remove from V all minor parallelotopes on which $\hat{f}$ degenerates, and stick the boundaries of the remaining parallelotopes in such a way that two points with a common image by $\hat{f}$ get together. Then, there arises a complex $\mathscr{V}$, which we shall call a guide complex. As shown by the diagram

$$\begin{tikzcd} V & & V \arrow[ll, "\hat{f}"'] \arrow[dl] \\ & \mathscr{V} \arrow[ul, "f"] & \end{tikzcd}$$

$\hat{f}$ induces a mapping f from $\mathscr{V}$ to V. The guide complex is similar to the complex used in combinatorial topology. A difference between the two is that the former is made from parallelotopes stuck together and not from simplexes. Anyway, $\mathscr{V}$ is a complex on which the local degree of mapping of f is everywhere defined, and the cyclotomic crystallographic group Γ operates on $\mathscr{V}$ as well. In addition, since $\hat{f}$ is homotopic to the identity map, the global degree of mapping of f is 1. On the other hand, the sign of the image by $\hat{f}$ of a minor parallelotope on which $\hat{f}$ does not degenerate in Figure 5 is nothing else than the local degree of mapping of f at an inner point of the minor parallelotope. Furthermore, the local degree of mapping of f is constant not only in an open parallelotope of the highest dimension but in all open parallelotopes of lower dimensions and on points that are produced by taking boundaries successively from minor parallelotopes of higher dimensions. Now we construct a fundamental domain $\Gamma\backslash\mathscr{V}$ rigorously by means of open parallelotopes, including lower-dimensional ones, and points. After that, we take the set of all images of f of members of the above $\Gamma\backslash\mathscr{V}$ and, based on the fact that the local degree of mapping of f is well defined along each member of $\Gamma\backslash\mathscr{V}$, define the sign of the image of a member of $\Gamma\backslash\mathscr{V}$ to be the local degree of mapping of f along the member. Maybe weight is a better expression than sign. The finite set of weighted parallelotopes thus obtained is a rigorous fundamental domain $\Gamma\backslash V$, because of the fact that the sum of local degrees of mapping of f at inverse images of a point is equal to the global degree of mapping of f. Whenever this fundamental domain is applied, the idea of the proof stated in §6 is completely justified.

2. When we explained in §6 that the reciprocity law is recognized as an evident fact, we used the expression, "β-division points with a common sign which are lined up in the direction of each side and are placed in number equal to multiples of n". Since this is rather coarse, a supplement should be given here. Among the sides of parallelotopes in the deformed fundamental domain in the left-hand side of Figure 5, there are long and short ones. The short ones come from short vectors joined to longer zigzag lines as in III of Figure 4. Precisely speaking, the word "each side" in the above quotation means only a long side. So, for instance, our logic does not hold for the parallelotope which has 0 as a vertex and has no long sides. Since, on the other hand, β-division points with a common sign ordered in the direction of a long side are counted by dividing the side into n equal parts, there can occur irregular β-division points in the neighborhood of ends of short segments. But, such irregularity is not of a very

bad nature. As a matter of fact, it is proved that, if β is screened satisfactorily by congruence and sign conditions and if the absolute value of β is sufficiently large, then $(\alpha/\beta)_n$ depends only on the argument of β, or, in general, on the tuple of arguments of images of β by all embeddings of F into $\mathbf{C}$. In addition, it is proved that $(\alpha/\beta)_n$ is locally constant in the space of such tuples except for a nowhere dense set. This result and the fact that every tuple has an arbitrarily close approximation by the argument tuple of the nth power of an integer entail $(\alpha/\beta)_n = 1$. In this way, the proof contains a qualitative change.

3. Another technical point concerns the intersection of the deformed fundamental domain and the parallelotopes which have been placed in the original crystal structure. Figure 2 shows that infinitely many images of P by the cyclotomic crystallographic group Γ cover the vector space. Provided that P is deformed into the figure as on the left-hand side of Figure 5, one may ask if the domain after the deformation intersects one of σP $(\sigma \in \Gamma,\ \sigma \neq 1)$. As a matter of fact, our proof does not work well if the deformed domain intersects that σP that does not touch P along a side. But, fortunately, we can conclude that, after multiplying α by the nth power of an integer if necessary, the intersection of the closures of the deformed domain and σP coincides with the intersection of closures of P and σP, provided that P and σP do not touch along a side. Accordingly, the intersection in question is either one point or empty, and this separation theorem saves the proof. Intuitively, this theorem is quite probable and actually easily proved in many concrete cases, but its general proof is presently not in a very elegant form. The technical difficulty as mentioned at the end of §6 here attains its peak. To improve the situation, a notation that conveniently expresses zigzag lines in a space is desired most of all.

8. Epilogue

1. A few words on the symmetric reciprocity law of the power residue symbol. What we call symmetric reciprocity in the present article is the well-known formula

$$(\alpha/\beta)_n(\beta/\alpha)_n^{-1} = \prod_{\mathfrak{p}|np_\infty} \left(\frac{\alpha,\beta}{\mathfrak{p}}\right)_n .$$

The symbol on the right-hand side is called the norm residue symbol, but its definition will not be given here. The product ranges over prime ideals dividing n and infinite places. Whenever the reciprocity law called asymmetric in §2 is proved, the above symmetric reciprocity can be deduced without difficulty. On the contrary, the symmetric reciprocity does not include the reciprocity for a general Kummer extension, for both α and β must be prime to n in the symmetric reciprocity. But, the symmetric reciprocity is more precise than the asymmetric reciprocity in the sense that it yields the equality between $(\alpha/\beta)_n$ and $(\beta/\alpha)_n$ when β is screened slightly. Thus, there is some difference between the two. In view of the Kummer extension, however, the asymmetric reciprocity is stronger.

2. Since the present article is entitled *A foundation of class field theory*, statements on the construction of class field theory cannot be avoided. As in 1 of §2, one can ask whether or not the reciprocity law for a general abelian extension, i.e., Assertion A, is a direct consequence of the reciprocity law for a Kummer extension, i.e., Assertion K, combined with the reciprocity law for a cyclotomic extension. This kind of problem has never been investigated carefully, but the answer can be given in a fairly routine way. The answer is "yes" if K/F is of an odd degree. In this case, Assertion A is obtained almost as a union of Assertion K and the reciprocity for a cyclotomic extension. There are various ways to see this. To give an outline of an example, assume, without loss of generality, that K/F is a cyclic extension of degree q, a power of an odd prime, and denote by ζ a primitive qth root of unity so that $K(\zeta)/F(\zeta)$ gives rise to a Kummer extension. Then, by twisting this Kummer extension slightly, we can construct another Kummer extension $K^*/F(\zeta)$ such that the equality $(\frac{K^*/F(\zeta)}{\mathfrak{a}}) = 1$ for an ideal $\mathfrak{a}$ of F, regarded as an ideal of $F(\zeta)$, implies $(\frac{K/F}{\mathfrak{a}}) = 1$. This means that Assertion A holds for K/F. The field K^* can be constructed from $K(\zeta)/F(\zeta)$ by a simple mechanical operation but is no longer abelian over F. If q is a power of 2, a field like K^* can also be constructed. But, in this case, ζ must be a root of unity whose order is a higher power of 2 than q. Moreover, the construction of K^* is not quite simple either but requires a more powerful device. As such a device, we may take the local-global principle which says that the quadratic form $\alpha x^2 + \beta y^2 = 1$ $(\alpha, \beta \in F)$ has a global solution in F whenever it has a solution everywhere locally in F. This principle is also called Hasse's principle and is the same as the norm theorem for a relatively quadratic extension. As long as the degree of K/F is even, a similar device is needed regardless of which way we might continue.

Hasse's principle is important in the equivalence theory of quadratic forms, and it was one of the fundamental theorems in the most difficult, quadratic case in Furtwängler's theory which includes a proof of the reciprocity law of the power residue symbol with a prime degree. It is interesting that such an essential assertion indicates the difference between the real reciprocity law for a general abelian extension and a mere union of the reciprocities for Kummer and cyclotomic extensions. From this point of view, we may understand that the contemporary, widely-known construction of class field theory is a too troublesome way to prove the first step of the general norm theorem. The proof of the local-global principle for $\alpha x^2 + \beta y^2 = 1$ must be independent of field extensions, because it is an assertion purely within the basic field. Although several proofs of the principle without field extension seem to be known, it is likely that there are still many things to do. In the rational case, the principle is proved very transparently by means of Minkowski's lattice point theorem, as originally pointed out by Legendre. This proof would be a very nice one, if it could be generalized.

3. One more comment. Viewed historically, the quadratic reciprocity concerning rational integers was formalized at the time of Euler, and Gauss proved it. After that, Gauss found an appropriate way to handle the biquadratic reciprocity in $\mathbf{Q}(\sqrt{-1})$, and its proof, together with the proof of the cubic reciprocity law in $\mathbf{Q}(\sqrt{-3})$, was first published by Eisenstein. Gauss did not publish any proof of biquadratic reciprocity, but one of his posthumous manuscripts did include a proof that was based on his own idea, which is rather similar to that given in this article and is actually geometric but is not sufficiently generalizable because it requires exact counts of lattice points in spatial figures. The method in this article is suitable for our purposes, since it contains, as its significance, an approximative approach as stated in 2 of §7 and does not pursue exact numbers of points to the very end. Gauss himself, as well as his successors, did not eagerly continue geometric investigations of the reciprocity law, but number theory turned mainly in the algebraic direction. After Gauss's genus theory of quadratic forms, Kummer greatly developed the theory of power residues in connection with extension fields. These results were made well-understandable by virtue of Dedekind's ideal theory. Hilbert presented a guiding outline of class field theory, and, following it, Furtwängler and Takagi brought class field theory and the reciprocity law of power residue symbols to their first definitive forms, with close relations with each other. Then Artin found the reciprocity law for abelian extensions. As mentioned at the beginning of §1, this discovery made it possible to summarize the entire class field theory in a very simple principle, Assertion A. But, what Artin did was not to give a simple proof to it but to derive it from other basic theorems of class field theory. After that, Galois cohomology theory was developed and class field theory was polished, in particular, due to the contributions of Herbrand and Tate. In the present class field theory, thus completed, the reciprocity law of the power residue symbol is derived as a special case from general theorems which are valid for all cases. As is realized by the fact that quadratic reciprocity was a major source of the remarkable development of classical number theory, the theory of power residues has an outstanding importance in number theory and is incomparably beautiful as well. The endeavor to complete the theory of power residues finally produced class field theory. This is a quite happy ending. But, one thing to be noticed is that, in the process of the research, people were perhaps dominated by the belief that power residues and extension fields are mutually inseparable. This kind of belief has the possibility of being strengthened to a belief that number theory is the theory of extension fields, including nonabelian ones. If, however, one regards the reciprocity law as being an assertion within a field and tries to prove it without going through the extension fields, then, as explained in the present article, it is proved in a geometric way in terms of intuitive properties of spatial figures only by means of tools that already existed at the time of Euler. This fact might have been rather difficult to find in spite of its simplicity but is almost obvious once thought of. So, let us assume the reciprocity law of the power residue symbol to be an easy fact. Then, Gauss's contribution is still significant because of his lemma as well as the discovery that gave a foundation of the theory (5 of §3). But, the post-Gauss development should be given a whole new evaluation from the viewpoint that the proof of the reciprocity law of the power residue symbol was the original and proper aim. The real weight of this article is not on a foundation of class field theory but on the point that a substantial part of the knowledge of number theory after Gauss was not absolutely necessary in order to prove the reciprocity law of the power residue symbol, which was a particularly important problem in number theory.

In old times, it was rather natural to treat power residues without applying field extensions. Such investigations are, however, mainly related to quadratic residues and are not well generalized even in the case where some of them concern higher residues. As stated above in connection with Gauss's posthumous manuscript, the idea explained in 2 of §7 enables a simple hint to be applicable to general cases and is one of the characteristic features of the present article. Because of its presence, that proof of the quadratic reciprocity concerning rational integers which is obtained by the method in this article does not coincide with any one of the proofs given by Gauss.

4. Literature. There are very few references that are closely related to this article. So, it is hard to provide a bibliography in the usual style. On the other hand, a significant number of papers must be listed if all the works on power residues and on class field theory are regarded as related to this article. For these reasons, we add here some short topics on the literature but not a list.

The paper in which Gauss introduced complex integers and founded the theory of biquadratic residues is *Theoria residuorum biquadraticorum*, I, II, *Complete works, Vol.* 2. Regarding Eisenstein's papers in which he proved the cubic and biquadratic reciprocity, as well as papers of Kummer, Furtwängler, etc., concerning the subsequent development of the theory, a list is given in Hasse's *Bericht*. The posthumous manuscript of Gauss concerning biquadratic residues is *Zur Theorie der biquadratischen Reste, Complete works, Vol.* 2. Apart from it, *Habicht*, Math. Ann. **139** (1960) is one paper in which power residues with a higher degree than 2 is treated geometrically. A proof of Hasse's principle which applies Minkowski's lattice point theorem as referred to in 2 is written in Cassels, *Rational quadratic forms*, Academic Press, 1978.

In the above paper with a Latin title, Gauss said, "Not much remains desirable in the theory of quadratic residues." But, as mentioned at the end of 3, the ideas explained in this article are, even though restricted to the case of quadratic residues concerning rational integers, not completely included in the frame of Gauss's research.

Reference

*1. Richard Hill, *Ein geometrischer Beweis eines Reziprozitätsgetzes*, Mathematica Gottingensis, Schriftenreihe des Sonderforsschungsbereichs Geometrie und Analysis **31** (1993).

Translated by T. KUBOTA

Department of Mathematics, Nagoya University, Furo-cho, Chikusa-ku, Nagoya, Japan

*Added in Proof.