ON THE RELATIONS BETWEEN CLASS NUMBERS OF QUADRATIC NUMBER FIELDS

A. SCHOLZ

Very little is known about the odd factors of the class numbers of quadratic number fields. It seems as if from relation between fields, which can be expressed most clearly through their discriminants, hardly a relation between their class groups can be derived. For example one might think that if the class groups of two fields $\mathbb{Q}(\sqrt{a}\,)$ and $\mathbb{Q}(\sqrt{b}\,)$ are known, something can be said about the field $\mathbb{Q}(\sqrt{ab}\,)$ contained in the compositum $\mathbb{Q}(\sqrt{a}, \sqrt{b}\,)$ that goes beyond simple statements concerning the number of genera. But comparing class number tables will hardly lead to any connection between the odd factors of class numbers of three quadratic fields $\mathbb{Q}(\sqrt{a}\,)$, $\mathbb{Q}(\sqrt{b}\,)$, $\mathbb{Q}(\sqrt{c}\,)$; $abc = e^2$. In addition it is known that the odd component of the class group of the compositum $\mathbb{Q}(\sqrt{a}, \sqrt{b}\,)$ is the direct sum of the odd components of the fields $\mathbb{Q}(\sqrt{a}\,)$, $\mathbb{Q}(\sqrt{b}\,)$, $\mathbb{Q}(\sqrt{c}\,)$.[1] Thus it seems as if the three odd class number factors of the three quadratic number fields have nothing to do with each other. In fact one may state *conjectures* such as the following:

If the quadratic number fields with class number divisible by the odd prime number p have a density, then for triples of dependent quadratic number fields the densities with respect to divisibility and nondivisibility are the products of the individual densities.

Here we have ordered the fields with respect to their absolute discriminant and the product of the discriminants, respectively.

Or more strongly: if we fix *one* quadratic field $\mathbb{Q}(\sqrt{\delta}\,)$, then the other quadratic number fields come in pairs $\mathbb{Q}(\sqrt{\partial}\,)$, $\mathbb{Q}(\sqrt{\delta\partial}\,)$. In general, there will be no relation between their odd class groups.

There is one case, however, where such a relation holds. Let us take $\mathbb{Q}(\sqrt{-3}\,)$ as one of the three fields, and let us compare the class groups of the fields $\mathbb{Q}(\sqrt{\partial}\,)$ and $\mathbb{Q}(\sqrt{-3\partial}\,)$; then the following relation holds between the 3-class groups of these fields:

Theorem 1. *Let r denote the 3-rank of the class group of the imaginary field among $\mathbb{Q}(\sqrt{\partial}\,)$ and $\mathbb{Q}(\sqrt{-3\partial}\,)$, and s the 3-rank of the real field (thus there are $3^r - 1$ and $3^s - 1$ ideal classes of order 3, respectively), then we have*

$$s \le r \le s + 1.$$

If, for example, the complex number field $\mathbb{Q}(\sqrt{-\Delta}\,)$ has a class number not divisible by 3, then so does the real field $\mathbb{Q}(\sqrt{3\Delta}\,)$. If $\mathbb{Q}(\sqrt{-\Delta}\,)$ has a cyclic 3-class group ($r = 1$), then $\mathbb{Q}(\sqrt{3\Delta}\,)$ either has a cyclic 3-class group ($s = 1$) or its 3-class number is not divisible by 3 at all ($s = 0$) etc. Here it is irrelevant which of the

[1]Cf. the exposition by F. Pollaczek on pp. 534–535 in "Über die Einheiten relativ-abelscher Zahlkörper", Math. Zeitschr. **30** (1929), which is also valid for $l = 2$.

two discriminants is divisible by 3. Whether we have $s = r$ or $s = r - 1$ has to be determined in a different way.

We now come to the proof, and we will use the notation above; in addition we set $\mathbb{Q}(\sqrt{-\Delta}\,) = K$ and $\mathbb{Q}(\sqrt{3\Delta}\,) = C$. The direct application of class field theory to cubic number fields [2] shows that there exist exactly r independent[3] cubic (non-normal) number fields with discriminant $-\Delta$ which, when lifted to $\mathbb{Q}(\sqrt{-\Delta}\,)$, are cyclic unramified extensions of $\mathbb{Q}(\sqrt{-\Delta}\,)$. These r number fields are generated by elements of the form

$$\begin{aligned}\theta_\rho &= \sqrt[3]{a_\rho + b_\rho\sqrt{3\Delta}} + \sqrt[3]{a_\rho - b_\rho\sqrt{3\Delta}} \\ &= \theta'_\rho + \theta''_\rho = \sqrt[3]{\alpha'_\rho} + \sqrt[3]{\alpha''_\rho} \qquad (\rho = 1, \ldots, r).\end{aligned}$$

Thus $K(\theta_\rho)$ is class field and, after adjoining $\sqrt{-3}$, $CK(\theta_\rho) = CK(\theta'_\rho)$ is class field over $K(\sqrt{-3}\,) = CK$. Here θ_ρ may be replaced by θ'_ρ: in fact, since $\alpha'_\rho \cdot \alpha''_\rho$ is a cube (actually the cube of $\frac{p}{3}$ if θ_ρ satisfies the equation $x^3 - px - q = 0$), we get the same extension over CK by adjoining $\sqrt[3]{\alpha'_\rho}$, $\sqrt[3]{\alpha''_\rho}$ or $\sqrt[3]{\alpha'_\rho} + \sqrt[3]{\alpha''_\rho}$. It follows from the fact that $CK(\theta'_\rho)$ is class field that α'_ρ is a singular primary element for the exponent 3, i.e., an ideal cube and a cubic residue modulo $3^{3/2}$; conversely this is a sufficient condition for $CK(\theta'_\rho)$ to be unramified.[4] Now α'_ρ is an element of C. Thus if it is an ideal cube in CK it must already be an ideal cube in C since CK has degree 2 over C.

To each ideal group in K with index 3 there corresponds an ideal cube α'_ρ in C whose cube root generates the associated class field over CK. Here the elements $\alpha'_1, \alpha'_2, \ldots, \alpha'_r$ must be independent modulo cubes of elements of CK, or, equivalently due to arguments involving the degree, of elements of C, i.e., $\prod {\alpha'_\rho}^{a_\rho} = \gamma^3$ (γ in C) if and only if all $a_\rho \equiv 0 \bmod 3$: in fact their cube roots generate r cubic extensions that are independent over CK.

In an arbitrary number field we denote by

- Z the group of elements that are ideal cubes, and by Z_3 the group of cubes;
- J the class group, by J_3 the subgroup of cubes in J;
- E the unit group, and by E_3 its subgroup of cubes.

We will denote the order of the factor group A/B by $[A : B]$. Then we have

$$[Z : Z_3] = [J : J_3] \cdot [E : E_3].$$

Thus in the field C we have $[Z : Z_3] = 3^{s+1}$. On the other hand $[Z : Z_3] \geq 3^r$, since the $\alpha'_1, \alpha'_2, \ldots, \alpha'_r$ form an independent (but not necessarily complete) system of representatives for the factor group Z/Z_3. This implies

$$r \leq s + 1.$$

Now we apply the same reasoning to C and K with their roles reversed, where we have to observe that the cyclic unit group in C disappears in K, which means that we simply have $[Z : Z_3] = 3^r$. On the other hand we have $[Z : Z_3] \geq 3^s$ since

---

[2] See H. Hasse: *Arithmetische Theorie der kubischen Zahlkörper auf klassenkörpertheoretischer Grundlage*, Math. Z. **31** (1930), pp. 565–582; §4.

[3] Extensions are called independent if the degree of their compositum is the product of the degrees of the extensions.

[4] See e.g. Ph. Furtwängler: *Allgemeiner Existenzbeweis für den Klassenkörper eines beliebigen algebraischen Zahlkörpers*, Math. Ann. **63** (1907), S. 1–37.

the wealth of ideal classes of C has the same effect on K as above that of K on C. Thus also here we have $s \le r$.

This finishes the proof of our theorem. We did not need the decisive property of singular prime elements in CK for finding the estimate on the ranks of the class groups but only the property that they are ideal cubes. For deciding whether $r = s$ or $r = s + 1$, then we have to use the other property of singular elements, that of being primary (cubic residue modulo $3^{3/2}$). For this property, the scope narrowed by the relation $s \le r \le s+1$. For if we collect the independent ideal cubes from K and C into a system

$$\rho_1, \rho_2, \ldots, \rho_r; \ \sigma_1, \sigma_2, \ldots, \sigma_s, \ \varepsilon$$

where ε denotes the fundamental unit in C, then all elements except one (if the basis is suitably chosen) are used for forming the Hilbert 3-class fields of C and K. Either all the $\rho_1, \ldots, \rho_r$ are primary ($r = s$), or all the $\sigma_1, \ldots, \sigma_s, \varepsilon$ are ($r = s + 1$). The remaining element τ in C or K is not primary: first it is independent in CK from the other elements with respect to cubes of elements: for according to the theorem mentioned above (footnote 1) the 3-class group of CK is the direct product of the 3-class groups of K and C; thus there cannot exist any "cubic relation" among the $r + s + 1$ elements. Thus $CK(\sqrt[3]{\tau})$ is not an unramified abelian extension, but rather a class field with conductor $\mathfrak{f} \ne 1$; but since τ is an ideal cube, we have $1 \ne \mathfrak{f} \mid 3^{3/2}$ and thus $\tau \not\equiv \gamma^3 \bmod 3^{3/2}$ according to footnote 4.

If one starts looking for such an element τ in order to decide whether $r = s$ or $r = s+1$, then it is not necessary to perform the cubic residue test modulo $3^{3/2}$ in CK; in fact it is sufficient to check this in C or K, that is, in the field to which the element belongs. (In that field in which the number 3 is not an ideal square this boils down to investigating the cubic residue character modulo 9.) In fact, both in CK and $\mathbb{Q}(\sqrt{-3})$, the residue class group modulo $3^{3/2}$ does not contain any residues of order 9, which is clear in the case where 3 splits into prime ideals of degree 1 in C or K (whichever field is the one with the discriminant coprime to 3), and which can easily be checked by a little computation in the other case where 3 does not split. Thus a number that is not a cubic residue (mod $3^{3/2}$) in a subfield of CK cannot become a cubic residue (mod $3^{3/2}$) in CK.

The fact that we only have to compute in quadratic number fields clearly simplifies the investigation. If, for example, the fundamental unit of C is known and if it is not a cubic residue, then we already know that $r = s$. If the unit is a cubic residue, then both cases can occur, but in this case the class number of K is certainly divisible by 3 ($r > 0$); for if $s = 0$, then the element τ, which is not primary, must occur among the elements $\rho_1, \ldots, \rho_r$. – In the general case s can be determined if the ideal class group (with representatives) of K is known; conversely we can determine r if the ideal class group and the fundamental unit of C are known.

Submitted May 6, 1931.

Translated[5] *by Franz Lemmermeyer*

---

[5] I have replaced Scholz's notation P (a Greek Rho) for the field of rational numbers throughout by $\mathbb{Q}$.