THE DEVELOPMENT OF THE PRINCIPAL GENUS THEOREM

FRANZ LEMMERMEYER

Introduction

Genus theory belongs to algebraic number theory and, in very broad terms, deals with the part of the ideal class group of a number field that is 'easy to compute'. Historically, the importance of genus theory stems from the fact that it was the essential algebraic ingredient in the derivation of the classical reciprocity laws – from Gauß's second proof over Kummer's contributions up to Takagi's 'general' reciprocity law for p-th power residues.

The central theorem in genus theory is the principal genus theorem, which is hard to describe in just one sentence – readers not familiar with genus theory might want to glance into Section 2 before reading on. In modern terms, the principal genus theorem for abelian extensions $k/\mathbb{Q}$ describes the splitting of prime ideals of k in the genus field k_{gen} of k, which by definition is the maximal unramified extension of k that is abelian over $\mathbb{Q}$.

In this note we outline the development of the principal genus theorem from its conception in the context of binary quadratic forms by Gauß (with hindsight, traces of genus theory can be found in the work of Euler on quadratic forms and idoneal numbers) to its modern formulation within the framework of class field theory. It is somewhat remarkable that, although the theorem itself is classical, the name 'principal ideal theorem' ('Hauptgeschlechtssatz' in German) was not used in the 19th century, and it seems that it was coined by Hasse in his Bericht [28] and adopted immediately by the abstract algebra group around Noether. It is even more remarkable that Gauß doesn't bother to formulate the principal genus theorem except in passing: after observing in [25, §247] that duplicated classes (classes of forms composed with themselves) lie in the principal genus, the converse (namely the principal genus theorem) is stated for the first time in §261:

> si itaque omnes classes generis principalis ex duplicatione alicuius classis provenire possunt (quod revera semper locum habere in sequentibus demonstrabitur), ...[1]

The actual statement of the principal genus theorem is somewhat hidden in [25, §286], where Gauß formulates the following

> Problem. Given a binary form $F = (A, B, C)$ of determinant D belonging to a principal genus: to find a binary form f from whose duplication we get the form F.

It strikes us as odd that Gauß didn't formulate this central result properly; yet he knew exactly what he was doing [25, §287]:

[1] if therefore all classes of the principal genus result from the duplication of some class (and the fact that this is always true will be proved in the sequel), ...

> Since by the solution of the problem of the preceding article it is clear that any properly primitive (positive) class of binary forms belonging to the principal genus can be derived from the duplication of any properly primitive class of the same determinant, ...

and he clearly saw the importance of this result:

> We believe that these theorems are among the most beautiful in the theory of binary forms, especially because, despite their extreme simplicity, they are so profound that a rigorous demonstration requires the help of many other investigations.

Gauß's theory of quadratic forms was generalized in several completely different directions:

(1) The theory of n-ary quadratic forms over fields, which was cultivated by Hermite, Smith, and Minkowski, and blossomed in the 20th century under the hands of Hasse, Witt, Siegel, and others.[2]
(2) The arithmetic of algebraic tori encompasses the theory of binary quadratic forms: see Shyr [72, 73] for a presentation of Gauß's theory in this language, and Ono [62] for a derivation of the principal genus theorem using results from Shyr's thesis.
(3) The theory of forms of higher degree, in particular cubic forms. We will be content with mentioning only two contributions to the algebraic theory of cubic forms: Eisenstein proved several results on cubic forms that nowadays would be presented in the language of cyclic cubic fields (see [40] for a modern interpretation of composition of cubic forms à la Kneser); Manin [54] studied cubic forms from the viewpoint of obstructions to the local-global principle, and his ideas led to profound insights in modern arithmetic geometry (see Skorobogatov [75]).
(4) The theory of quadratic and, later, general algebraic number fields, with Kummer, Dirichlet, Dedekind, and Weber being responsible for the transition from forms to ideal classes in number fields.

This article is restricted to the genus theory of number fields; for a related survey with an emphasis on the quadratic case, but sketching generalizations of the genus concept e.g. in group theory, see Frei [19].

I. Genus Theory of Quadratic Forms

1. Prehistory: Euler, Lagrange and Legendre

There are hardly any traces of genus theory in the mathematical literature prior to Gauß's Disquisitiones. What can be found, in particular in Euler's work, are results and conjectures that later were explained by genus theory.

One such conjecture was developed between Goldbach and Euler: on March 12, 1753, Goldbach wrote to Euler [18, Letter 166] that if p is a prime $\equiv 1 \bmod 4d$, then p can be represented as $p = da^2 + b^2$. Euler replies on March 23/April 3 [18, Letter 167]:

[2]See Jones [42], Lam [48], and O'Meara [61] for n-ary forms, and Buell [6] for the binary case; Venkov [85] gives a very readable presentation of Gauß's results close to the original.

> Ich habe auch eben diesen Satz schon längst bemerket und bin von der Wahrheit desselben so überzeugt, als wann ich davon eine Demonstration hätte.[3]

He then gives the examples

$$\begin{aligned} p = 4\cdot 1m+1 &\quad\Longrightarrow\quad & p = \ aa+bb \\ p = 4\cdot 2m+1 &\quad\Longrightarrow\quad & p = 2aa+bb \\ p = 4\cdot 3m+1 &\quad\Longrightarrow\quad & p = 3aa+bb \\ p = 4\cdot 5m+1 &\quad\Longrightarrow\quad & p = 5aa+bb \quad \textit{etc.} \end{aligned}$$

and remarks that he can prove the first claim, but not the rest.[4] Euler then goes on to observe that the conjecture is only true in general when a and b are allowed to be rational numbers, and gives the example $89 = 4\cdot 22+1$, which can be written as $89 = 11(\frac{5}{2})^2 + (\frac{9}{2})^2$ but not in the form $11a^2+b^2$ with integers a, b. Thus, he says, the theorem has to be formulated like this:

Conjecture 1. *Si $4n+1$ sit numerus primus, et d divisor ipsius n, tum iste numerus $4n+1$ certo in hac forma $daa+bb$ continentur, si non in integris, saltem in fractis.*[5]

Euler also studied the prime divisors of a given binary quadratic form x^2+ny^2 (in the following, we will always talk about 'proper' divisors of quadratic forms, that is, we assume that $p \mid x^2+ny^2$ with $\gcd(x,y)=1$), and observed that those not dividing $4n$ are contained in half of the possible residue classes modulo $4n$ coprime to $4n$: for example, the prime divisors of x^2+5y^2 are contained in the residue classes $1, 3, 7, 9 \bmod 20$; no prime congruent to $11, 13, 17, 19 \bmod 20$ divides x^2+5y^2 without dividing x and y.[6] Now, as Euler knew (and he used this in his 'solution' of the cubic Fermat equation), odd primes dividing x^2+ny^2 can be represented by the same quadratic form if $n=3$, and he also knew that this property failed for $n=5$. He then saw that the primes $p \equiv 1, 9 \bmod 20$ could be represented[7] as $p = x^2+5y^2$ with $x, y \in \mathbb{N}$, whereas $p \equiv 3, 7 \bmod 20$ could be written as $2x^2+2xy+3y^2$ with $x, y \in \mathbb{Z}$. His first guess was that this would generalize as follows: the residue classes containing prime divisors of x^2+ny^2 could be associated uniquely with a reduced quadratic form of the same discriminant as x^2+ny^2. For example, the reduced forms associated to $F = x^2+30y^2$ are the forms D satisfying $D = F$, $2D = F$, $3D = F$ and $5D = F$, where $2D = F$ refers to $D = 2r^2+15s^2$, $3D = F$ to $3r^2+10s^2$, and $5D = F$ to $D = 5r^2+6s^2$. Each of these forms has different classes of divisors.

As Euler [16, p. 192] found out, however, $n = 39$ provides a counterexample: he comes up with three classes of forms

---

[3] I have known this very theorem for quite a long time, and I am just as convinced of its truth as if I had its demonstration.

[4] Later he found a proof for the case $p = 3a^2+b^2$; the other two cases mentioned here were first proved by Lagrange.

[5] If $4n+1$ is a prime number, and d a divisor of this n, then that number $4n+1$ is certainly contained in the form $daa+bb$, if not in integers, then in fractions.

[6] Euler [16, p. 210] expressed this by saying that primes (except $p = 2, 5$) dividing x^2+5y^2 have the form $10i \pm 1$, $10i \pm 3$, where the plus sign holds when i is even, and the minus sign when i is odd.

[7] At this stage, he had already studied Lagrange's theory of reduction of binary quadratic forms.

> Hinc igitur patet omnino dari tria genera divisorum:[8]
>
> $$1)\ D = F, \qquad 2)\ 3D = F, \qquad [3)]\ 5D = F.$$

These three kinds of divisors are $D = F = r^2+39s^2$; $D = 3r^2+13s^2$ (note that $3D = (3r)^2 + 39s^2$, which explains Euler's notation $3D = F$); and $D = 5r^2 + 2rs + 8s^2$. He then observes that the divisors of the first and the second class share the same residue classes modulo 156; the prime $61 = 3 \cdot 4^2 + 13 \cdot 1^2$ belonging to the second class can be represented rationally by the first form since $61 = (\frac{25}{4})^2 + 39(\frac{3}{4})^2$.

Euler and Lagrange. One of the results in which Euler comes close to genus theory is related to a conjecture of Euler that was shown to be false by Lagrange; it appears in [15]. In his comments on Euler's algebra, Lagrange [47, p. 156–157] writes

> Euler, dans un excellent Mémoire imprimé dans le tome IX des *nouveaux Commentaires de Pétersbourg*, trouve par induction cette règle, pour juger la résolubilité de toute equation de la forme
>
> $$x^2 - Ay^2 = B,$$
>
> lorsque B est un nombre premier; c'est que l'équation doit être possible toutes les fois que B sera de la forme $4An + r^2$, ou $4An + r^2 - A$;[9]

For example, $-11 = 4 \cdot 3 \cdot (-1) + 1^2$, and $-11 = 1^2 - 3 \cdot 2^2$. Similarly, $-2 = 4 \cdot 3 \cdot (-2) + 5^2 - 3$ and $-2 = 1^2 - 3 \cdot 1^2$. Euler's main motivation for this conjecture were numerical data, but he also had a proof that $p = x^2 - ay^2$ implies $p = 4an + r^2$ or $p = 4an + r^2 - a$. In fact, he writes $x = 2at + r$, $y = 2q + s$, and finds that $p = x^2 - ay^2 = 4am + r^2 - as^2$ for some $m \in \mathbb{Z}$. If s is even, then $-as^2$ has the form $4am'$, and if s is odd, we find $-as^2 = -4am'' - a$. This proves the claim.

As Lagrange pointed out, however, Euler's conjecture is not correct, and he came up with the following counterexample: the equation $x^2 - 79y^2 = 101$ is not solvable in integers, although $101 = 4An + r^2 - A$ with $A = 79$, $n = -4$ and $r = 38$.

Whether Euler ever heard about Lagrange's counterexample is not clear; based on Euler's experience in such matters it is not unreasonable to suspect that he probably would have reacted in the same way as in the other cases above, namely by replacing the representation in integers by representation in rational numbers. This would have led to the following

Conjecture 2. *If $p \nmid 4a$ is a prime of the form $4an + r^2$ or $4an + r^2 - a$, then $p = x^2 - ay^2$ for rational numbers x, y.*

As we shall see, this conjecture is equivalent to Gauß's principal genus theorem.

Euler and Genus Theory. Antropov [1, 2, 3] has tried to make a case for the claim that the concept of genera is due to Euler. In [1], he writes

> It seems to have gone unnoticed that Euler partitioned the set of the integral binary quadratic forms with a given discriminant into classes, which he called "genera".

[8] Thus from here it becomes clear that there are altogether three kinds of divisors:

[9] M. Euler, in an excellent Memoir printed in vol. IX of the *New Commentaries of Petersburg*, finds by induction this rule for determining the solvability of every equation of the form $x^2 - Ay^2 = B$, where B is a prime number: the equation must be possible whenever B has the form $4An + r^2$, or $4An + r^2 - A$;

Euler did use the word 'genus', as we have seen, for distinguishing between certain kinds of quadratic forms; however, Euler uses both genus ("ad genus tertium pertinentis") and class ("ad tertiam classem pertinet") when talking about what Antropov perceives as a 'genus' of quadratic forms.

Fueter, in his preface [22, p. xiii], praises Euler's contributions as follows:

> Man kann sagen, daß eigentlich alle Bausteine der Zahlentheorie dieses Gebietes in den EULERSCHEN Abhandlungen schon bereitgestellt wurden, und es nur der Meisterhand eines GAUSS bedurfte, um sie zu dem Gebäude der Theorie der quadratischen Formen zusammenzufügen.[10]

A more realistic view was later offered by Weil, who – referring to Euler's papers on idoneal numbers – wrote ([89, p. 224])

> They are [...] ill coordinated with one another, and some of the formulations and proofs in them are [...] confused and defective ...

One must not forget, however, that Euler only had isolated results on (divisors of) numbers represented by quadratic forms, and that it may be unfair to judge his work in the light of the insight provided by Gauß, who subsumed Euler's (and Lagrange's) results into just a few theorems (reciprocity, class group, principal genus theorem) within his theory of quadratic forms.

Legendre. As for Legendre's contribution, Dirichlet [12, p. 424] writes

> Les formes différentes qui correspondent au déterminant quelconque D, sont divisées par M. GAUSS en genres, qui sont analogues à ce que LEGENDRE appelle groupes des diviseurs quadratiques.[11]

Legendre's 'diviseurs quadratiques' of a binary quadratic forms are the reduced nonequivalent quadratic forms of the same 'determinant'; to each of these classes he associates 'diviseurs lineaires', namely the linear forms $ax+b$ with the property that the primes represented by the 'diviseur quadratique' are contained in the arithmetic progression $ax + b$ (see [49, Art. 212] for the 8 diviseurs quadratiques of $x^2 + 41y^2$ and the 6 diviseurs lineaires corresponding to each of them).

2. GAUSS

Let us start by briefly recalling Gauß's definitions. In Section V of his Disquisitiones Arithmetica, he studies binary quadratic forms $F(x, y) = ax^2 + 2bxy + cy^2$ that are occasionally denoted by (a, b, c); the *determinant* of F is $D = b^2 - ac$. An integer n is said to be *represented* by F is there exist integers x, y such that $n = F(x, y)$. A form (a, b, c) is *ambiguous* if $a \mid 2b$, and *primitive* if $\gcd(a, b, c) = 1$.

The following theorem proved in §229 is the basis for the definition of the genus of a binary quadratic form:

[10] One might argue that essentially all the building blocks of the number theory of this area had been provided by EULER, and that it only took the masterly hand of GAUSS to join them to the edifice of the theory of binary quadratic forms.

[11] The different forms that correspond to some determinant D are partitioned by Mr. GAUSS into genera, which are analogous to what LEGENDRE calls groups of quadratic divisors.

> Let F be a primitive binary quadratic form with determinant D, and let $p \mid D$ be prime. Then the numbers not divisible by p that can be represented by F agree in that they are either all quadratic residues of p, or they are all nonresidues.

For $p = 2$ the claim is correct but trivial. If $4 \mid D$, however, then the numbers represented by f are all $\equiv 1 \bmod 4$, or all $\equiv 3 \bmod 4$. Similarly, if $8 \mid D$, the numbers lie in exactly one of the four residue classes $1, 3, 5$ or $7 \bmod 8$.

Gauß adds without proof the remark that there is no such pattern for odd primes *not* dividing the discriminant:

Observation. *If it were necessary for our purposes we could easily show that numbers representable by the form F have no such fixed relationship to a prime number that does not divide D* [12]

except for the residue classes modulo 4 and 8 of representable odd numbers in case D is odd:

I. If $D \equiv 3 \bmod 4$, then the odd n that can be represented by F are all $\equiv 1 \bmod 4$ or all $\equiv 3 \bmod 4$.
II. If $D \equiv 2 \bmod 8$, then the odd n that can be represented by F are all $\equiv \pm 1 \bmod 8$ or all $\equiv \pm 3 \bmod 8$.
III. If $D \equiv 6 \bmod 8$, then the odd n that can be represented by F are all $\equiv 1, 3 \bmod 8$ or all $\equiv 5, 7 \bmod 8$.

Gauß uses this observation to define characters of primitive quadratic forms (§230); for example, to the quadratic form $(7, 0, 23)$ he attaches the *total character* $1, 4; R7; N23$ because the integers represented by $7x^2 + 23y^2$ are $\equiv 1 \bmod 4$, quadratic residues modul 7, and quadratic nonresidues modulo 23. Gauß observes that if (a, b, c) is a primitive quadratic form, then $p \mid b^2 - ac$ implies $p \nmid \gcd(a, c)$, so the character of primitive forms can be determined from the integers a and c, which of course are both represented by (a, b, c). Finally he remarks that forms in the same class have the same total character, which allows him to consider them as characters of the classes.

Now Gauß collects classes of forms of given determinant into genera: a genus is simply the set of all classes with the same total character. The principal genus is the genus containing the principal class (the class containing the principal form $(1, 0, -D)$).

Next on Gauß's agenda (§234 – §256) is the definition of the composition of forms, orders, genera,[13] and classes of forms. The next three articles (§257 – §259) are devoted to the determination of the number of ambiguous classes.

In §261 Gauß proves the *first inequality* of genus theory: at least half of all possible total characters do not occur. This is a consequence of the 'ambiguous class number formula'. §262 is reserved for a demonstration that the first inequality implies the quadratic reciprocity law.

---

[12] Übrigens würden wir, wenn es zum gegenwärtigen Zwecke notwendig wäre, leicht beweisen können, daß die durch F darstellbaren Zahlen zu keiner in D nicht aufgehenden Primzahl in einer derartigen festen Beziehung stehen.

[13] This terminology is apparently taken from biology. C. Linne classified the living organisms into kingdoms (plants and animals), classes, orders, genera, and species. Kummer used the German expression 'Gattung' for Gauß's 'genus', but in the long run the translation 'Geschlecht' prevailed.

In §266, Gauß begins a long excursion into the theory of ternary quadratic forms $Ax^2+2Bxy+Cy^2+2Dxz+2Eyz+Fz^2$. After discussing the reduction of ternary quadratic forms, he remarks that ternary forms represent both integers (by substituting integers for x, y, z) and quadratic forms (by putting e.g. $x = at + bu$, $y = ct + du$, $z = et + fu$ for variables t and u).

After having studied the representations of binary quadratic forms by ternary forms, Gauß returns to binary quadratic forms in §286 and proves the principal genus theorem: every form F in the principal genus is equivalent to $2f$ for some form f of the same determinant as F. This immediately implies the *second inequality* of genus theory in §287: at least half of all possible total characters do in fact occur. Finally, in §303, Gauß characterizes Euler's idoneal numbers using genus theory.

Ambiguous Forms and Classes. In his Marburg lectures, Hasse [30, p. 158] writes

> Die in diesem Zusammenhang nicht sehr glückliche Bezeichnung "ambig" stammt von Gauß.[14]

Gauß, however, wrote in Latin and used 'forma anceps' to denote an ambiguous quadratic form; apparently Hasse confused the disquisitiones with Maser's translation, where 'anceps' is translated as 'ambig'.[15]

The actual story of the word ambiguous is given by Dedekind [11, §58, p. 139]:

> In his lectures Dirichlet always used the word *forma anceps*, which I have kept when I prepared the first edition (1863); in the second and third edition (1871, 1879), [...] I called them *ambiguous forms* following Kummer, who used this notation in a related field;

apparently there were complaints about the word, and in the fourth edition he replaces 'ambiguous' by 'twosided' (zweiseitig in German).

As a matter of fact, the expression 'ambiguous' was not at all Kummer's invention: it was used in the form 'classe ambiguë' by Poullet Delisle in his French translation of the disquisitiones, which appeared in 1807. By the time Kummer started studying number theory, the Latin edition of the disquisitiones must have been next to impossible to get; we know that Eisenstein's copy of the disquisitiones was in French (see Weil [90]), and it seems reasonable to assume that Kummer studied the same edition.

Ternary Forms. Gauß used his theory of ternary quadratic forms to prove the principal genus theorem, and derived Legendre's theorem (as well as the 3-squares theorem[16]) from the same source. Arndt [4] and later Dedekind [11, §158] and Mansion [55] realized that Legendre's theorem is sufficient for proving the principal genus theorem, which simplified the theory considerably (see [50, Chap. 2]). Unfortunately, however, Legendre's theorem does not seem to suffice for deriving the 3-squares theorem, but Deuring [10, VII, §9] (see also Weil [89, III, App. II; p. 292–294]) sketched a very beautiful proof using the theory of quaternion algebras. Venkov (1927; see [85]) used Gauß's theory of ternary quadratic forms to give an arithmetic proof of Dirichlet's class number formula for negative discriminants $-m$

[14]The term "ambiguous", whose usage in this connection is somewhat unfortunate, is due to Gauß.

[15]Clarke used 'ambiguous' in his English translation, and I. Adamson used 'ambig' in his English translation of Hilbert's Zahlbericht.

[16]Every positive integer not of the form $4^a(8b+7)$ can be written as a sum of three squares.

in which m is the sum of three squares. Shanks [70] used binary quadratic forms to develop his extremely clever factorization algorithm SQUFOF,[17] and Gauß's theory of ternary quadratic forms [71] for coming up with an algorithm for computing the 2-class group of complex quadratic number fields.

3. Dirichlet-Dedekind

According to a well known story (see Reichardt [65, p. 14]), Dirichlet never put Gauß's disquisitiones on the bookshelf but kept the copy on his desk and took it with him on journeys. Dirichlet's constant occupation with the disquisitiones provided him with the insight that allowed him to streamline and simplify Gauß's exposition, thereby making the disquisitiones accessible to a much wider audience.

In [12], Dirichlet replaces Gauß's notation aRp by $(a/p) = +1$, thus giving Gauß's characters the now familiar look. His main contribution in [12] was definitely the proof of the 'second inequality' of genus theory using analytic methods.[18]

Dirichlet presented the theory of binary quadratic forms in his lectures; his results on genus theory were added by Dedekind in the supplements IV (analytic proof) and X (arithmetic proof using Legendre's theorem). In §122, he defines an integer

$$\lambda = \#\{\text{odd primes dividing } D\} + \begin{cases} 0 & \text{if } D \equiv 1 \bmod 4 \\ 2 & \text{if } D \equiv 0 \bmod 8 \\ 1 & \text{otherwise,} \end{cases}$$

and in §123 he proves the first inequality of genus theory:

$$g \le 2^{\lambda-1}.$$

In §125, he gives Dirichlet's analytic proof of the existence of these genera, the second inequality of genus theory:

> Die Anzahl der wirklich existierenden Geschlechter ist gleich $2^{\lambda-1}$, und alle diese Geschlechter enthalten gleich viele Formenklassen.[19]

He also remarks that the second inequality would follow immediately from Dirichlet's theorem on the infinitude of primes in arithmetic progressions.

Dedekind returns to genus theory of binary quadratic forms in his supplement X: §153 gives the first inequality, §154 the quadratic reciprocity law, and in §155 he observes that the second inequality of genus theory (the existence of half of all the possible genera) is essentially identical with the principal genus theorem:

> Every class of the principal genus arises from duplication.

He then remarks

> Wir können hier unmöglich darauf eingehen, den Beweis mitzutheilen, welchen Gauss auf die Theorie der ternären quadratischen Formen gestützt hat; da dieses tiefe Theorem aber den schönsten Abschluss der Lehre von der Composition bildet, so können wir es uns nicht versagen, dasselbe auch ohne Hülfe der Dirichlet'schen

[17] SQUare FOrm Factorization.

[18] See Zagier [91] for a modern exposition.

[19] The number of existing genera is $2^{\lambda-1}$, and all these genera contain equally many classes of forms.

> Principien auf einem zweiten Wege abzuleiten, der zugleich die Grundlage für andere wichtige Untersuchungen bildet.[20]

His proof begins by showing that the following statement is equivalent to the principal genus theorem:

> If (A, B, C) is a form in the principal genus of determinant D, then the equation
>
> $$Az^2 + 2Bzy + Cy^2 = x^2$$
>
> has solutions in integers z, y, x such that x is coprime to $2D$. [21]

In §158 Dedekind gives a proof of the principal genus theorem based on Legendre's theorem (which, as he observes in a footnote in §158, belongs to the theory of ternary quadratic forms) and refers to Arndt [4] for a first proof of this kind.

Remark. The genus theory of Dirichlet and Dedekind is a genus theory of binary quadratic forms. Although Dedekind introduced ideals and maximal orders in number fields, he did not translate genus theory into his new language.

Dirichlet's analytic methods were used to prove the principal genus theorem by Kronecker [43] and de Séguier [68, p. 135–153; 333-334]. A proof based on Dedekind's criterion involving (1) was given by Pépin [63, p. 45].

Mertens [56] gave a new proof of the principal genus theorem built on Legendre's theorem. De la Vallée Poussin [84] and Mertens [57] found proofs based only on binary quadratic forms. See also Speiser [77].

Heine [32] studied quadratic forms over function fields of one variable; see also Bae & Koo [5] and Hellegouarch [33]. The 'genre principal' introduced by Serret [69] in his investigations of irreducible polynomials of degree p^μ over $\mathbb{F}_p[X]$ seems unrelated to the principal genus of Gauß.

Dirichlet [13], Smith [76], and Minnigerode [58] investigated binary quadratic forms with coefficients in $\mathbb{Z}[i]$. Speiser [78] developed genus theory for binary quadratic forms with coefficients from the ring of integers of an arbitrary number field.

II. Genus Theory of Quadratic Number Fields

4. Hilbert

Before Hilbert published his report on algebraic numbers, he worked on the arithmetic of quadratic extensions of $\mathbb{Q}(i)$ (Dirichlet fields) with the intention of

> extending the theory of Dirichlet's biquadratic number field in a purely arithmetic way to the same level that the theory of quadratic number fields has had since Gauss,

[20] It is impossible for us to communicate the proof, which Gauss has based on the theory of ternary quadratic forms; but since this deep theorem is the most beautiful conclusion of the theory of composition, we cannot help but derive this result, without the use of Dirichlet's principles, in a second way, which will also form the basis for other important investigations.

[21] Ist (A, B, C) eine Form des Hauptgeschlechtes der Determinante D, so ist die Gleichung

$$Az^2 + 2Bzy + Cy^2 = x^2 \tag{1}$$

stets lösbar in ganzen Zahlen z, y, x, deren letzte relative Primzahl zu $2D$ ist.

and the main tool for achieving this goal was, according to Hilbert, the notion of genera of ideal classes. [22]

Let $\mathbb{Z}[i]$ denote the ring of Gaussian integers, and let $\delta \in \mathbb{Z}[i]$ be a squarefree nonsquare. Hilbert considers the quadratic extension $K = \mathbb{Q}(\sqrt{\delta})$ of $k = \mathbb{Q}(i)$, computes integral bases, and determines the decomposition of primes.

For the definition of the genus Hilbert introduces the prototype of his norm residue symbol. For $\sigma \in k$ and λ a prime divisor $\neq (1+i)$ of the discriminant of K/k, Hilbert writes $\sigma = \alpha\nu$ as a product of a relative norm ν and some $\alpha \in \mathbb{Z}[i]$ not divisible by λ, and puts

$$\Big[\frac{\sigma}{\lambda : \delta}\Big] = \Big[\frac{\alpha}{\lambda}\Big],$$

where $[\,\cdot\,/\,\cdot\,]$ is the quadratic residue symbol in $\mathbb{Z}[i]$. The definition for $\lambda = 1+i$ is slightly more involved.

Then Hilbert defines the character system of an ideal $\mathfrak{a}$ in $\mathcal{O}_K$ as the system of signs

$$\Big[\frac{\sigma}{\lambda_1 : \delta}\Big], \ldots, \Big[\frac{\sigma}{\lambda_s : \delta}\Big],$$

where $\lambda_1, \ldots, \lambda_s$ denote the ramified primes. The character system of ideals only depends on their ideal class, and classes with the same character system are then said to be in the same genus. The principal genus is the set of ideal classes whose character system is trivial. The principal genus theorem is formulated in [35, §4]:

> Each ideal class in the principal genus is the square of some ideal class.[23]

Hilbert then determines the number of genera, derives the quadratic reciprocity law, and finally gives an arithmetic proof of the class number formula for $\mathbb{Q}(i, \sqrt{m})$ and $m \in \mathbb{Z}$. He apparently has not yet realized that his symbols $\left[\frac{\sigma}{\lambda:\delta}\right]$ are 'norm residue' symbols, or that the quadratic reciprocity law can be expressed by a product formula.

He takes these steps in the third section of his Zahlbericht, which deals with the theory of quadratic number fields. He calls an integer n a norm residue[24] at p in $\mathbb{Q}(\sqrt{m})$ if m is a square or if for all $k \ge 1$ there exist integers $x, y \in \mathbb{Z}$ such that $n \equiv x^2 - my^2 \bmod p^k$. Then he defines the norm residue symbol by

$$\Big(\frac{n\,,\,m}{p}\Big) = \begin{cases} +1 & \text{if } m \text{ is a norm residue at } p \text{ in } \mathbb{Q}(\sqrt{m}) \\ -1 & \text{otherwise.} \end{cases}$$

Hilbert uses the norm residue symbol to define characters on ideal classes and defines the principal genus to consist of those ideal classes with trivial character system. In §68, he employs ambiguous ideals and his Satz 90 to prove that quadratic number fields with exactly one ramified prime have odd class number, and then deduces the quadratic reciprocity law in §69. In §72 he proves the principal genus theorem:

---

[22] The complete quotation from [35] reads: Die vorliegende Abhandlung hat das Ziel, die Theorie des Dirichletschen biquadratischen Zahlkörpers auf rein arithmetischem Weg bis zu demjenigen Standpunkt zu fördern, auf welchem sich die Theorie der quadratischen Körper bereits seit Gauss befindet. Es ist hierzu vor allem die Einführung des Geschlechtsbegriffs sowie eine Untersuchung derjenigen Einteilung aller Idealklassen notwendig, welche sich auf den Geschlechtsbegriff gründet.

[23] Eine jede Idealklasse des Hauptgeschlechtes ist gleich dem Quadrat einer Idealklasse.

[24] I will adapt the following convention: an element is a norm residue *modulo* $\mathfrak{a}$ if it is congruent to a norm modulo $\mathfrak{a}$, and a norm residue at $\mathfrak{p}$ if it is congruent to norms modulo any power $\mathfrak{p}^k$.

> In einem quadratischen Körper ist jede Klasse des Hauptgeschlechts stets gleich dem Quadrat einer Klasse (Gauss).[25]

The proof uses a reduction technique reminiscent of Lagrange; the solvability of the 'norm equation' $n = x^2 - my^2$ for $x, y \in \mathbb{Q}$ is equivalent to the fact that the ternary quadratic form $x^2 - my^2 - nz^2$ nontrivially represents 0 in integers, and Hilbert explicitly refers to Lagrange when he states the following special case of 'Hasse's norm theorem':

> Satz 102. Wenn n, m zwei ganze rationale Zahlen bedeuten, von denen m keine Quadratzahl ist, und die für jede beliebige Primzahl w die Bedingung
>
> $$\left(\frac{n\,,\,m}{w}\right) = +1$$
>
> erfüllen, so ist die Zahl n stets gleich der Norm einer ganzen oder gebrochenen Zahl α des Körpers $k(\sqrt{m}\,)$.[26]

(Note that $k(\sqrt{m}\,)$ denotes the quadratic number field k one gets by adjoining $\sqrt{m}$ to the field of rational numbers.)

The ambiguous class number formula is proved afterwards, and finally Hilbert gives a second proof of the principal genus theorem using Dirichlet's analytic techniques.

Remark. With Hilbert, the transition from Gauß's genus theory of binary quadratic forms to the corresponding theory of quadratic extensions is complete. Distinctive features of Hilbert's presentation are

(1) the central role of the ambiguous class number formula; the cohomological kernel of these results was recognized only much later;
(2) the introduction of norm residue symbols and the formulation of the reciprocity law as a product formula.

Although Hilbert saw that the norm residue symbol for the 'infinite prime' of $\mathbb{Q}$ (he wrote it as $(\frac{n,m}{-1})$; see [36, §70]) would simplify the presentation, he chose not to use it. These symbols became necessary when he replaced $\mathbb{Q}$ by arbitrary base fields k in his article [38] on class field theory.

5. Weber

In the third volume of his algebra [88, §108], Weber gives an account of genus theory that shows Hilbert's influence: while Weber does not include the theory of the quadratic Hilbert symbol, he realizes the importance of the concept of norm residues.

He fixes a modulus $m \in \mathbb{N}$, considers a natural number S divisible by m, and forms[27] the multiplicative group Z of rational numbers coprime to S, that is, the set of all $\frac{a}{b}$ with $a, b \in \mathbb{Z}$ and $\gcd(a, S) = \gcd(b, S) = 1$. The kernel of the natural map $Z \longrightarrow (\mathbb{Z}/m\mathbb{Z})^\times$ is the group M of all elements of Z that are congruent to 1 mod m, and Weber observes that $(Z : M) = \phi(m)$.

---

[25] In a quadratic number field, each class of the principal genus is the square of a class (Gauss).

[26] Theorem 102. If n, m denote two rational integers, where m is a nonsquare, and if for any prime w the condition

$$\left(\frac{n\,,\,m}{w}\right) = +1$$

is satisfied, then n is the norm of a (not necessarily integral) number α of the field $k(\sqrt{m}\,)$.

[27] Presumably this is influenced by Hensel.

Now let $\mathcal{O}$ denote an order of a quadratic number field k (Weber writes Q instead of $\mathcal{O}$) such that the prime factors of the conductor of $\mathcal{O}$ divide S; in particular, the discriminant Δ of $\mathcal{O}$ is only divisible by primes dividing S. The set of integers $a \in \mathbb{Z}$ for which there is an $\omega \in \mathcal{O}$ with $N\omega \equiv a \bmod m$ form a subgroup A of M, the group of norm residues modulo m of $\mathcal{O}$.

In order to simplify the presentation, let $A\{m\}$ denote the group of norm residues modulo m. Weber [88, §107] observes that if $m = m_1m_2$ with $\gcd(m_1, m_2) = 1$, then $(Z : A\{m\}) = (Z : A\{m_1\})(Z : A\{m_2\})$, thereby reducing the computation of the index $(Z : A\{m\})$ to the case of prime powers m.

In [88, §108], he proves

$$(Z : A\{p^t\}) = \begin{cases} 1 & \text{if } p \nmid \Delta \\ 2 & \text{if } p \mid \Delta \end{cases}$$

if p is an odd prime, and

$$(Z : A\{2^t\}) = \begin{cases} 1 & \text{if } \Delta \equiv 1 \bmod 4,\ \Delta \equiv 4, 20 \bmod 32, \\ 2 & \text{if } \Delta \equiv 8, 12, 16, 24, 28 \bmod 32, \\ 4 & \text{if } \Delta \equiv 0 \bmod 32. \end{cases}$$

If r is norm residue modulo m for any modulus m coprime to r, then r is called an absolute norm residue, and the set of all such $r \in Z$ forms a group R ([88, §109]). As a consequence of his index computations above, Weber records

$$(Z : R) = 2^\lambda,$$

where λ is the number of discriminant divisors of Δ. A divisor δ of Δ is called a discriminant divisor if both δ and Δ/δ are discriminants.

Weber [88, §109] defines the genus of an ideal as the set of all ideals $\mathfrak{a}$ coprime to Δ whose norms $N\mathfrak{a}$ are in the same coset of Z/R, and observes that equivalent ideals have the same genus. The principal genus is the group of all ideals coprime to Δ such that $N\mathfrak{a} \in R$. He shows that the existence of primes that are quadratic nonresidues modulo Δ implies that the number g of genera satisfies the inequality

$$g \le \frac{1}{2}(Z : R), \tag{2}$$

and that the existence of such primes is equivalent to the quadratic reciprocity law (once more we can observe the close connection between quadratic reciprocity and the first inequality). The fact that we have equality in (2) is proved in [88, §113] using Dirichlet's analytic methods.

Remark. Weber's presentation of the genus theory of orders in quadratic number fields was taken up (to some degree) in Hecke's textbook. Observe that the 'localization' of the necessary index calculations is much more visible in Weber's than in Hilbert's treatment. Moreover, these index formulas are intimately related to Gauß's observation on p. 6.

6. Hecke

Hecke's 'Vorlesungen' [31] contain a masterful exposition of algebraic number theory, including the genus theory of (the maximal orders of) quadratic fields. After the explosion of events in algebraic number theory of the 1920s, genus theory

was thrust into the background as local methods gradually replaced genus theory in the foundation of class field theory.

Hecke's presentation of genus theory in quadratic fields k with discriminant d combines known with new features:

- Hecke uses class groups in the strict sense; already Hilbert [36, §83–84] had seen that this simplifies the exposition of genus theory because some of the statements "can be expressed in a simpler way by using the new notions".[28]
- Hecke uses Weber's index computation for norm residues, but restricts his attention right from the start to norm residues modulo d.
- Hecke gives a new and very simple definition of genera: two ideals $\mathfrak{a}$ and $\mathfrak{b}$ coprime to d are said to belong to the same genus if there exists an $\alpha \in k^\times$ such that $N\mathfrak{a} = N\mathfrak{b} \cdot N(\alpha)$; note that $N(\alpha) > 0$.

As a corollary of genus theory and the index calculations Hecke obtains the following characterization:

Proposition 1. *Let k be a quadratic number field with discriminant d. An ideal $\mathfrak{a}$ coprime to d is in the principal genus if and only if one of the following equivalent conditions is satisfied:*

(1) *$\mathfrak{a}$ is equivalent in the strict sense to the square of some ideal $\mathfrak{b}$;*
(2) *$(\frac{N\mathfrak{a},d}{p}) = +1$ for all primes $p \mid d$;*
(3) *$N\mathfrak{a} = N(\alpha)$ for some $\alpha \in k^\times$;*
(4) *$N\mathfrak{a} \equiv N(\alpha) \bmod d$ for some $\alpha \in k^\times$.*

Hecke – of course – gives the analytic proof of the existence of genera:

> Die Tatsache, daß die Anzahl der Geschlechter g genau $= 2^{t-1}$ ist, wird nun am bequemsten mit Benutzung transzendenter Methoden [...] bewiesen[29]

and remarks, after having given the 'fundamental theorem on genera':

> Gauß hat diesen Satz zuerst gefunden und für ihn einen rein arithmetischen Beweis gegeben.[30]

Remark. Olga Taussky [81, §5] characterizes the principal genus using matrices.

7. Euler's Conjectures Revisited

In this section we will show that Euler's Conjecture 1 and his 'corrected' Conjecture 2 follow from genus theory. Assume that n is a positive squarefree integer and that $p \equiv 1 \bmod 4n$ is prime. Then $(p/p_i) = +1$ for all primes $p_i \mid n$, which by quadratic reciprocity (note that inverting Legendre symbols is no problem since $p \equiv 1 \bmod 4$) implies $(d_i/p) = (p_i/p) = +1$, where d_i are the prime discriminants[31] dividing $d = \operatorname{disc} \mathbb{Q}(\sqrt{n}\,)$. Applying the following proposition with $a = -n$ then shows that the Goldbach-Euler conjecture is true (at least for squarefree n):

---

[28] ... und einige [dieser Tatsachen] erhalten bei Verwendung der neuen Begriffe sogar noch einen einfacheren Ausdruck.

[29] The fact that the number g of genera is $= 2^{t-1}$ can be proved most conveniently by using transcendental methods [...].

[30] Gauß has discovered this theorem and gave a purely arithmetic proof.

[31] A prime discriminant is a discriminant of a quadratic number field that is a prime power.

Proposition 2. *Let a be a squarefree integer $\ne 1$, $k = \mathbb{Q}(\sqrt{a}\,)$ a quadratic number field with discriminant d, and $p > 0$ a prime not dividing d. Then the following conditions are equivalent:*

1. *there exist $x, y \in \mathbb{Q}$ with $p = x^2 - ay^2$;*
2. *we have $(d_i/p) = 1$ for all prime discriminants d_i dividing* $\operatorname{disc} k$*;*
3. *we have $p\mathcal{O}_k = \mathfrak{p}\mathfrak{p}'$, and $\mathfrak{p}$ is equivalent to the square of an ideal in $\mathcal{O}_k$ in the strict sense.*

Proof. Condition (1) says that the norm of a prime ideal $\mathfrak{p}$ above p is the norm of an element, which by Proposition 1.3 implies that $\mathfrak{p}$ is in the principal genus, which is (3). Similarly, if p does not divide d, then the Legendre symbols (d_i/p) essentially coincide with Hilbert symbols $(\frac{p,d}{p_i})$, where p_i is the unique prime dividing d_i, and this time we see that $\mathfrak{p}$ is in the principal genus by Proposition 1.2. The claim that (3) $\Longrightarrow$ (1) is proved by simply taking norms. □

Let us now have a look at Lagrange's counterexample to Euler's original conjecture in the light of Gauß's (or rather Hecke's) genus theory. First we observe that 79 is the smallest natural number a such that the class group of $\mathbb{Q}(\sqrt{a}\,)$ is strictly larger than the genus class group, and the fact that Lagrange didn't give a smaller counterexample suggests a connection between Euler's conjecture and genus theory.

In fact, if we replace the condition $x, y \in \mathbb{Z}$ in $p = x^2 - Ay^2$ by $x, y \in \mathbb{Q}$, then Euler's conjecture is true and essentially equivalent to the principal genus theorem. To the best of my knowledge, however, this has not been noticed before, neither by Lagrange (who pointed out that Euler's conjecture was false), nor by Legendre (who proved a related result on the solvability of $ax^2 + by^2 + cz^2$, which contains criteria for the solvability of $-c = aX^2 + bY^2$ in rational numbers as a special case), nor by anyone else for that matter. The following lemma shows the connection of Euler's criterion with something more familiar:

Lemma 1. *Let a be a squarefree integer $\ne 1$, $k = \mathbb{Q}(\sqrt{a}\,)$ a quadratic number field with discriminant d, and $p > 0$ a prime not dividing d. Then the following conditions are equivalent:*

1. *there exist $n, r \in \mathbb{Z}$ such that $p = 4an + r^2$ or $p = 4an + r^2 - a$;*
2. *we have $(d_i/p) = 1$ for all prime discriminants d_i dividing* $\operatorname{disc} k$*.*

The proof is a simple exercise using the quadratic reciprocity law; Proposition 2 then shows that Euler's Conjecture 2 is in fact just a version of the principal genus theorem of quadratic forms or fields.

Remark. In his preface to Euler's Opera Omnia I–4 Fueter [22, p. xiii] remarks that Euler's observation in [17] that only half of all possible prime residue classes mod $4n$ may yield prime factors of $x^2 + ny^2$ is equivalent to Gauß's result that at most half of all possible genera exist. Gauß had already remarked in [25, §151] that there is a gap in Euler's proof.

Edwards [14, p. 274] observes

> The case $D = 79$ is one that Gauß frequently uses as an example (DA arts 185, 186, 187, 195, 196, 198, 205, 223)

and speculates that Gauß's interest in this discriminant may have been sparked by Lagrange's counterexample.

III. Genus Theory and Higher Reciprocity Laws

8. Kummer

Kummer's motivation for creating a genus theory for Kummer extensions over $\mathbb{Q}(\zeta)$, where ζ is a primitive ℓ-th root of unity, was his quest for a proof of the reciprocity law for ℓ-th powers: call an $\alpha \in \mathbb{Z}[\zeta]$ primary if α is congruent to a nonzero integer modulo $(1-z)^2$ and if $\alpha\overline{\alpha}$ is congruent to an integer modulo ℓ. For primary and coprime integers $\alpha, \beta \in \mathbb{Z}[\zeta]$, Kummer had conjectured the reciprocity law $(\alpha/\beta) = (\beta/\alpha)$, where $(\,\cdot\,/\,\cdot\,)$ is the ℓ-th power residue symbol. When everything else had failed (in particular cyclotomic methods like Gauß and Jacobi sums), he turned to Gauß's genus theory.

Let us fix some notation: ℓ will denote an odd prime, ζ a primitive ℓ-th root of unity, $\lambda = 1-\zeta$, and $\mathfrak{l} = (\lambda)$ the prime ideal in $k = \mathbb{Q}(\zeta)$ above ℓ. Let M denote the set of all $\alpha \in k^\times$ coprime to $\mathfrak{l}$.

The generalization of Gauß's theory of genera of quadratic forms to Kummer extensions $k(\sqrt[\ell]{\alpha}\,)/k$ looks quite natural to mathematicians who are familiar with the interpretation of the theory of binary quadratic forms as an arithmetic of ideals in quadratic number fields; although Kummer never worked out such a theory, he was aware that his ideal numbers could be generalized to this situation (with the same problems as over Kummer extensions of cyclotomic fields: primes dividing the conductor of the ring had to be excluded).

Armed with this insight, it is clear that the quadratic extensions $\mathbb{Q}(\sqrt{d}\,)$ had to be replaced by Kummer extensions, and that representability of primes by binary quadratic forms corresponded to being norms of prime ideals in ideal classes.[32] But what are the right analogs of Gauß's characters? As Kummer eventually realized, these characters could be constructed using 'differential logarithms'.

Assume that $\alpha \in \mathbb{Z}[\zeta]$ satisfies $\alpha \equiv 1 \bmod \lambda$, and write it as $\alpha = f(\zeta)$ for some polynomial $f \in \mathbb{Z}[X]$; replace X by the function e^v, evaluate the r-th derivative of $\log f(e^v)$ with respect to v at $v = 0$, and call the result $\mathcal{L}^r(\alpha)$ (Kummer wrote $\frac{d_0^r \log f(e^v)}{dv^r}$ instead; the subscript 0 at d_0^r indicates that the derivative should be evaluated at $v = 0$). For $1 \le r \le \ell - 2$, the resulting integer modulo ℓ does not depend on the choice of f; with a little bit more care it can be shown that a similar procedure gives a well defined result even for $r = \ell - 1$.

It was noticed by Takagi and Hasse that Kummer's differential logarithms can (and should) be described algebraically; here is a short summary of the most basic properties of the $\mathcal{L}^r$ (see [51, Chapter 14]):

Proposition 3. *Kummer's differential logarithms*[33] $\mathcal{L}^r$ $(1 \le r \le p-1)$ *have the following properties:*

i) $\mathcal{L}^r(\alpha\beta) = \mathcal{L}^r(\alpha) + \mathcal{L}^r(\beta)$ *for all* $\alpha, \beta \in M$
ii) $\mathcal{L}^r(\alpha^\sigma) = \chi(\sigma)^r \mathcal{L}^r(\alpha)$, *where* $\chi : \mathrm{Gal}(k/\mathbb{Q}) \longrightarrow \mathbb{F}_\ell$ *is the cyclotomic character defined by* $\zeta^\sigma = \zeta^{\chi(\sigma)}$;
iii) $\mathcal{L}^r(\alpha) = \mathcal{L}^r(\beta)$ *for all* $\alpha, \beta \in M$ *with* $\alpha \equiv \beta \bmod \lambda^{r+1}$;

[32] We replace Kummer's language by Dedekind's. We also use the notation familiar from Galois theory; instead of denoting the conjugates of $\alpha = f(\zeta)$ by $f(\zeta^r)$ as Kummer did, we let $\sigma : \zeta \longmapsto \zeta^r$ act on α.

[33] I prefer differential logarithm to logarithmic derivative since 3.i) resembles the functional equation of the logarithm and not the Leibniz rule.

iv) $\mathcal{L}^r(1+\lambda^r) = (-1)^r r!$.

Kummer introduced his differential logarithms in [45, p. 493] in connection with Gauss sums and observes in a special case that $\mathcal{L}^r(\alpha^\sigma) = (-1)^r\mathcal{L}^r(\alpha)$, where σ denotes complex conjugation. This special case of Proposition 3.ii) immediately implies that $\mathcal{L}^r(\alpha) = 0$ for all real $\alpha \in k$ whenever r is odd; in particular, $\mathcal{L}^{2r+1}(\varepsilon) = 0$ for all real units in $\mathbb{Z}[\zeta]$.

Put $K = \mathbb{Q}(\zeta_\ell)$, fix an integer $\mu \in \mathbb{Z}[\zeta_\ell]$ and consider the Kummer extension $L = K(\sqrt[\ell]{\mu})$. Kummer's "integers in w" were elements of $\mathcal{O}[w]$, where $w = \sqrt[\ell]{\mu}$ and $\mathcal{O} = \mathbb{Z}[\zeta_\ell]$; observe that $\mathcal{O}[w] \neq \mathcal{O}_L$ in general even when μ is squarefree. Next he introduces integers $z_j = (1-\zeta)(1-\mu)/(1-w\zeta^j) \in \mathcal{O}[w]$ as well as the ring $\mathcal{O}_z = \mathcal{O}[z_0, z_1, \dots, z_{\ell-1}]$ and observes that $\mathcal{O}_z \subseteq \ell\mathcal{O}[w] \subseteq \mathcal{O}_z$. On [p. 676-677] he discusses the decomposition law, excluding primes dividing $\lambda\mu$.

Assume that $\mathfrak{p}$ is a prime ideal in $\mathbb{Z}[\zeta]$ and let h denote the class number. Then $\mathfrak{p}^h = (\pi)$, and we can try to define $\mathcal{L}^r(\mathfrak{p})$ by the equation $h\mathcal{L}^r(\mathfrak{p}) = \mathcal{L}^r(\pi)$. Unfortunately, the values of $\mathcal{L}^r(\pi)$ depend on the choice of π in general, although not always: since $\mathcal{L}^{2r+1}(\varepsilon_j) = 0$ for all real units ε_j and all $0 \le r \le \rho = \frac{1}{2}(\ell-1)$, and since moreover $\mathcal{L}^{2r+1}(\zeta) = 0$ for all $1 \le r \le \rho$, we can define $\mathcal{L}^{2r+1}(\mathfrak{p}) = \frac{1}{h}\mathcal{L}^{2r+1}(\pi)$.

This allows Kummer to define ρ characters χ_3, χ_5, $\dots$, $\chi_{\ell-2}$ on the group of ideals in $\mathcal{O}_z$ prime to $\ell \cdot \operatorname{disc}(L/K)$ by putting

$$\chi_{2r+1}(\mathfrak{P}) = \zeta^S, \quad S = \mathcal{L}^{2r+1}(N_{L/K}\mathfrak{P}).$$

To these characters he adds

$$\chi_{\ell-1}(\mathfrak{P}) = \zeta^S, \quad S = \frac{1-N\mathfrak{P}}{\ell}.$$

Now let $\mathfrak{p}_1, \dots, \mathfrak{p}_t$ denote the primes different from (λ) that are ramified in L/K. For each such prime Kummer defines a character

$$\psi_j(\mathfrak{P}) = \left(\frac{N_{L/K}\mathfrak{P}}{\mathfrak{p}_j}\right).$$

Here $\mathfrak{p} = N_{L/K}\mathfrak{P}$ is an ideal in $\mathbb{Z}[\zeta]$, $\mathfrak{p}^h = (\pi)$ is principal, and if we insist in taking π primary, then the symbol $(\pi/\mathfrak{p}_j)$ only depends on $\mathfrak{P}$. We therefore put $(N_{L/K}\mathfrak{P}/\mathfrak{p}_j) = (\pi/\mathfrak{p}_j)^{h^*}$, where h^* is an integer such that $h^*h \equiv 1 \bmod \ell$.

All in all there are now $\rho + t$ characters, and these can be shown to depend only on the ideal class of $\mathfrak{P}$ ([45, p. 748]). The ideal classes with trivial characters form a subgroup C^z_{gen} in $\mathrm{Cl}^z(L)$, the class group of the order $\mathcal{O}_z$, and C^z_{gen} is called the principal genus. The quotient group $\mathrm{Cl}^z_{\text{gen}}(L/K) = \mathrm{Cl}^z(L)/C^z_{\text{gen}}$ is called the genus class group, and the main problem is to determine its order. This problem is solved by invoking ambiguous ideal classes (see [45, p. 751]):

> Die Anzahl aller wirklich vorhandenen Gattungen ist nicht größer, als die Anzahl aller wesentlich verschiedenen, nicht äquivalenten ambigen Klassen.[34]

On the next 40 pages, Kummer [45, p. 752–796] shows that there are exactly $\ell^{\rho+t-1}$ ambiguous ideal classes; this is quite a surprising result, because the ambiguous class number formulas the we are familiar with all contain a unit index as a factor. The amazing thing is that it is Kummer's 'weird' choice of the order

[34]The number of existing genera is not greater than the number of all essentially different nonequivalent ambiguous classes.

he is working in eliminates this index! By working in an order with a nontrivial conductor Kummer is actually able to simplify genus theory considerably.

As the number of pages he spends on this topic shows, he had to work hard nonetheless. For counting the number of ambiguous ideal classes he comes up with his integers in u, coinciding with the integers in w in the case where μ is a prime ideal power. Actually what he is doing is writing the h-th power of μ as a product of t principal prime powers, adjoining their ℓ-th roots u_j to $\mathcal{O}_z$, and then showing that ambiguous prime ideals in $\mathcal{O}_z$ become principal in the extension $\mathcal{O}_u = \mathcal{O}_w[u_1, \ldots, u_t]$ in such a way that their generators can be made into elements of $\mathcal{O}_w$ through multiplication by powers of the u_j ([45, p. 768]).

To illustrate this result, take $k = \mathbb{Q}(\sqrt{15})$ with the ambiguous ideals $\mathfrak{2} = (2, 1+\sqrt{15})$, $\mathfrak{3} = (3, \sqrt{15})$ and $\mathfrak{5} = (5, \sqrt{15})$: these become principal in the ring $\mathbb{Z}[\sqrt{3}, \sqrt{5}]$ as $\mathfrak{2} = (\sqrt{3}+\sqrt{5})$, $\mathfrak{3} = (\sqrt{3})$ and $\mathfrak{5} = (\sqrt{5})$, and multiplying these generators with $\sqrt{3}$ produces integers in $\mathbb{Z}[\sqrt{15}]$. Had Kummer demanded that the u_j be primary, the u_j would generate a subfield of the genus class field of K/k, and his result would say that ambiguous ideal classes become principal there: this is a near miss that even Hilbert did not follow out (although it may have inspired his Satz 94 on the capitulation of ideals in unramified cyclic extensions).

Next Kummer [45, p. 796] obtains the first inequality of genus theory, namely the fact that there are at most $\ell^{\rho+t-1}$ genera (Kummer writes λ instead of ℓ):

> Die Anzahl der wirklich vorhandenen Gattungen ist nicht größer als der ℓ-te Theil aller bloß angebbaren Gattungen oder Gesamtcharaktere.[35]

He notes, however, that this is not good enough to prove the reciprocity law: imitating Gauß's second proof only gives a distinction between ℓ-th power residues and nonresidues, but is not powerful enough to distinguish between e.g. $(\alpha/\mathfrak{p})_\ell = \zeta$ and $(\alpha/\mathfrak{p})_\ell = \zeta^2$.

Kummer closes this gap by proving the second inequality in some special cases. To this end, he has to study norm residues modulo powers of $(1-\zeta)$ in the Kummer extensions $\mathbb{Q}(\zeta, \sqrt[\ell]{\mu})/\mathbb{Q}(\zeta)$. His first result is that if a number $\alpha \in \mathbb{Z}[\zeta]$ is a norm from $\mathcal{O}_w$, then ([45, p. 805])

$$\mathcal{L}^1(\alpha)\mathcal{L}^{\ell-1}(\mu) + \mathcal{L}^2(\alpha)\mathcal{L}^{\ell-2}(\mu) + \mathcal{L}^{\ell-1}(\alpha)\mathcal{L}^1(\mu) \equiv 0 \bmod \ell. \tag{3}$$

This is an amazing result: the left hand side of (3) is an element of $\mathbb{F}_p$, and this element vanishes if α is a norm from $\mathcal{O}_w$. Hilbert later realized that the left hand side is just the additively written norm residue symbol at the prime $\mathfrak{p}$ above p.

On p. 808 Kummer shows that condition (3) is equivalent to

$$\left(\frac{\varepsilon}{\mu}\right) = \left(\frac{\eta}{\alpha}\right),$$

where ε and η are units such that $\varepsilon\alpha$ and $\eta\mu$ are primary.

If $\mathfrak{p}$ is a prime ideal in $\mathcal{O}_k$ such that $(\varepsilon/\mathfrak{p}) = 1$ for all units $\varepsilon \in \mathcal{O}_k^\times$, then $\mathfrak{p}$ is called a prime ideal of the second kind, and of the first kind otherwise.

The first special case is obtained on p. 811: if $t = 1$, and if the ramified prime ideal is of the first kind, then there are exactly ℓ^ρ genera. On p. 817, he obtains a similar result for certain Kummer extensions with exactly two ramified primes.

[35] The number of existing genera is not greater than the ℓ-th part of all possible genera or total characters.

This turns out to be sufficient for proving the reciprocity laws, but before he does so, he applies these reciprocity laws to derive the general principal genus theorem on p. 825:

> Die Anzahl der wirklich vorhandenen Gattungen der idealen Zahlen in z ist genau gleich dem ℓ-ten Theile aller Gesamtcharaktere. [36]

9. Hilbert

Hilbert's Zahlbericht[37] consists of five parts: the foundations of ideal theory, Galois theory, quadratic number fields, cyclotomic fields, and Kummer extensions, and the first four parts are still considered to be standard topics in any introduction to algebraic number theory. The fifth part, clearly the most difficult section of the Zahlbericht, did not make it into any textbook and was soon superseded by the work of Furtwängler and Takagi. Yet it is this chapter that I regard to be the Zahlbericht's main claim to fame: it reflects Hilbert's struggle with digesting Kummer's work, of finding a good definition of the norm residue symbol, and of incorporating Kummer's isolated results on genus theory of Kummer extensions into a theory which is on a par with the genus theory of binary quadratic forms in Gauß's Section V of the Disquisitiones.

The quadratic norm residue symbol $(\frac{n\,,m}{p})$ is defined to be $+1$ if m is a square or if n is congruent modulo any power of p to the norm of a suitable integer from $\mathbb{Q}(\sqrt{m}\,)$, and $(\frac{n\,,m}{p}) = -1$ otherwise. This Hilbert symbol can be expressed using Legendre symbols; in [37, Satz 13] Hilbert derives the formula

$$\Big(\frac{\nu,\mu}{\mathfrak{p}}\Big) = \Big(\frac{(-1)^{ab}\rho\sigma}{\mathfrak{p}}\Big)$$

for the Hilbert symbol for primes $\mathfrak{p} \nmid 2$ in number fields k, where $\mathfrak{p}^a \parallel \mu$, $\mathfrak{p}^b \parallel \nu$, and $\nu^a\mu^{-b} = \rho\sigma^{-1}$ for integers $\rho, \sigma \in \mathcal{O}_k$ coprime to $\mathfrak{p}$.

For defining the ℓ-th power norm residue symbol for odd primes ℓ, Hilbert proceeds in the opposite direction. Let $v_\mathfrak{p}$ denote the $\mathfrak{p}$-adic valuation, i.e.' let $v_\mathfrak{p}(\alpha)$ be the maximal power of $\mathfrak{p}$ dividing α. For $\mu, \nu \in k^\times$ put $a = v_\mathfrak{p}(\mu)$ and $b = v_\mathfrak{p}(\nu)$. Then $\nu^a\mu^{-b} = \rho\sigma^{-1}$ for integers $\rho, \sigma \in \mathcal{O}_k$ such that $v_\mathfrak{p}(\rho) = v_\mathfrak{p}(\sigma) = 0$. Now define

$$\Big(\frac{\nu,\mu}{\mathfrak{p}}\Big)_\ell = \Big(\frac{\rho}{\mathfrak{p}}\Big)_\ell \Big(\frac{\sigma}{\mathfrak{p}}\Big)_\ell^{-1}$$

for all prime ideals $\mathfrak{p}$ not dividing ℓ.

The definition of the norm residue symbol for primes ideals $\mathfrak{p} \mid \ell$ is much more involved; in his Zahlbericht, Hilbert only considers the case $k = \mathbb{Q}(\zeta_\ell)$ and uses Kummer's differential logarithms in the case $\ell \ge 3$: for $\mu \equiv \nu \equiv 1 \bmod \ell$, he puts (compare Kummer's result (3))

$$\Big(\frac{\nu,\mu}{\mathfrak{l}}\Big)_\ell = \zeta^S \quad \text{with } S \;=\; \mathcal{L}^1(\nu)\mathcal{L}^{\ell-1}(\mu) - \mathcal{L}^2(\nu)\mathcal{L}^{\ell-2}(\mu) \pm \ldots - \mathcal{L}^{\ell-1}(\nu)\mathcal{L}^1(\mu),$$

and then extends it to μ, ν coprime to ℓ by

$$\Big(\frac{\nu,\mu}{\mathfrak{l}}\Big)_\ell \;=\; \Big(\frac{\nu^{\ell-1},\mu^{\ell-1}}{\mathfrak{l}}\Big)_\ell.$$

[36] The number of existing genera in the theory of ideal numbers in z is equal to the ℓ-th part of all total characters.

[37] It was almost immediately translated into French (1909); meanwhile, there also exist translations into Romanian (1997) and English (1998).

Hilbert's genus theory goes like this:[38] let $k = \mathbb{Q}(\zeta_\ell)$, and assume that the class number h of k is not divisible by ℓ. Consider the Kummer extension $K = k(\sqrt[\ell]{\mu})$. Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_t$ denote the primes that are ramified in K/k (including infinite ramified primes if $\ell = 2$). For each ideal $\mathfrak{a}$ in $\mathcal{O}_k$, write $N_{K/k}\mathfrak{a}^h = \alpha\mathcal{O}_k$; the map

$$\alpha \longmapsto X(\alpha) = \left\{ \left(\frac{\alpha, \mu}{\mathfrak{p}_1}\right), \ldots, \left(\frac{\alpha, \mu}{\mathfrak{p}_t}\right) \right\}$$

induces a homomorphism $\psi : \mathrm{Cl}(K) \longrightarrow {\mathbb{F}_l}^t / X(E_k)$ by mapping an ideal class $[\mathfrak{a}]$ to $X(\alpha)^{h^*} X(E_k)$, where h^* is an integer with $h^* h \equiv 1 \bmod \ell$. Its kernel $C_{\mathrm{gen}} = \ker \psi$ is called the principal genus, and the quotient group $\mathrm{Cl}_{\mathrm{gen}}(K) = \mathrm{Cl}(K)/C_{\mathrm{gen}}$ the genus class group of K.

In [36, Satz 150] Hilbert generalizes Gauß's observation on p. 6 by proving that the index of norm residues modulo $\mathfrak{p}^e$ in the group of all numbers coprime to $\mathfrak{p}$ is 1 if $\mathfrak{p}$ is unramified, and equal to ℓ if $\mathfrak{p} \neq \mathfrak{l}$ is ramified or if $\mathfrak{p} = \mathfrak{l}$ and $e > \ell$.

Next Hilbert shows that his symbol defined in terms of power residue symbols actually is a norm residue symbol in [36, Satz 151].

Following Gauß, Hilbert then proves the inequality $g \leq a$ between the number of genera and ambiguous ideal classes ([36, Hilfssatz 34]), then proves the reciprocity law $\prod_v (\frac{a\,,\,b}{v}) = 1$ for the ℓ-th power Hilbert symbol and regular primes ℓ ([36, §160]), and finally derives the second inequality $g \geq a$ ([36, Satz 164]). This result is then used for proving the principal genus theorem in [36, Satz 166]:

> jede Klasse des Hauptgeschlechtes in einem regulären Kummerschen Körper K ist gleich dem Produkt aus der $1 - S$-ten symbolischen Potenz einer Klasse und einer solchen Klasse, welche Ideale des Kreiskörpers $k(\zeta)$ enthält.[39]

(Observe that this implies the familiar equality $C_{\mathrm{gen}} = \mathrm{Cl}(K)^{1-\sigma}$ if we work with ℓ-class groups.) Satz 167 finally shows that numbers in k that are norm residues at every prime $\mathfrak{p}$ actually are norms from K, and Hilbert concludes this section with the remark

> Damit ist es dann gelungen, alle diejenigen Eigenschaften auf den regulären Kummerschen Körper zu übertragen, welche für den quadratischen Körper bereits von Gauss aufgestellt und bewiesen worden sind.[40]

For connections between genus theory and reciprocity laws see also Skolem [74].

IV. Genus Theory in Class Field Theory

10. Furtwängler

In Furtwängler's construction of Hilbert class fields, the following theorem (see [23]) played a major role:

---

[38] We have taken the liberty of rewriting it slightly using the concept of quotient groups.

[39] every class of the principal genus in a regular Kummer field K is the product of the $1 - S$-th symbolic power of an ideal class and of a class containing ideals of the cyclotomic field $k(\zeta)$.

[40] Thus we have succeeded in transferring all those properties to the regular Kummer fields that already have been stated and proved for quadratic number fields by Gauß.

Theorem 1. *Let L/K be a cyclic unramified extension, σ a generator of the Galois group* $\mathrm{Gal}(L/K)$*, and let $N : \mathrm{Cl}(L) \longrightarrow \mathrm{Cl}(K)$ be the norm map on the ideal class groups. Then* $\ker N = \mathrm{Cl}(L)^{1-\sigma}$.

This almost looks like the vanishing of $H^{-1}(G, \mathrm{Cl}(L))$, but actually we have $H^{-1}(G, \mathrm{Cl}(L)) \neq 0$ in general; this is due to the difference between the relative norm

$$N_{L/K} : \mathrm{Cl}(L) \longrightarrow \mathrm{Cl}(K)$$

and the algebraic norm

$$\nu_{L/K} = 1 + \sigma + \sigma^2 + \ldots + \sigma^{(L:K)-1} : \mathrm{Cl}(L) \longrightarrow \mathrm{Cl}(L);$$

the connection between these two norms is the relation $\nu = j \circ N$, where $j : \mathrm{Cl}(K) \longrightarrow \mathrm{Cl}(L)$ is the transfer of ideal classes. This means that Furtwängler's principal theorem can't be translated easily into the cohomological language because ideal classes may capitulate. Furtwängler [24] used his principal genus theorem to study the capitulation of ideals in Hilbert 2-class fields of number fields with 2-class group isomorphic to $(2, 2)$.

Furtwängler also proved that, for cyclic extensions L/K of prime degree, an element $\alpha \in K^\times$ is a norm from L if and only if it is a norm residue modulo the conductor $\mathfrak{f}$ of L/K (Hasse's contribution was the interpretation of this result as a Local-Global principle). We will later see that this result can be expressed cohomologically as $H^{-1}(\mathrm{Gal}(L/K), C_L) = 1$, where C_L is the idèle class group; for this reason, Kubota [44] calls $H^1(C) = 0$ the principal genus theorem and credits Furtwängler for the 'fully idèle-theoretic' result in the case of Kummer extensions of prime degree.[41] Nakayama [59], on the other hand, claims that $H^1(C) = 0$ is 'merely the idèle-class analogue of Noether's principal genus theorem', while Chevalley [9] calls it the generalization of Hasse's principal genus theorem to normal extensions.

11. Takagi and Hasse

In this section we assume some familiarity with the classical version of class field theory. Let L/K be an extension of number fields and $\mathfrak{m}$ a modulus in K. Let $P^1\{\mathfrak{m}\}$ denote the set of principal ideals (α) in K with $\alpha \equiv 1 \bmod \mathfrak{m}$, and let $D_K\{\mathfrak{m}\}$ denote the group of ideals in K coprime to $\mathfrak{m}$, and let $D_K\{\mathfrak{m}\}$ denote the corresponding object for K. Then we call $H_{L/K}\{\mathfrak{m}\} = N_{L/K} D_L\{\mathfrak{m}\} \cdot P^1\{\mathfrak{m}\}$ the ideal group defined mod $\mathfrak{m}$ associated to L/K.

In the special case where $\mathfrak{m}$ is an integral ideal, such groups had been studied by Weber; in their theory of the Hilbert class field, Hilbert and Furtwängler defined infinite primes, and Takagi combined these two notions to create his class field theory.

Takagi called L a class field of K for the ideal group $H_{L/K}\{\mathfrak{m}\}$ if $(D_K\{\mathfrak{m}\} : H_{L/K}\{\mathfrak{m}\}) = (L : K)$. In order to show that abelian extensions are class fields, this equality has to be proved, and the proof is done in two steps:

(1) the First Inequality

$$(D_K\{\mathfrak{m}\} : H_{L/K}\{\mathfrak{m}\}) \leq (L : K),$$

[41] In [44], Kubota shows that the second inequality of class field theory is essentially a corollary of two of Furtwängler's results: the product formula for the Hilbert symbol (i.e., the reciprocity law), and the principal genus theorem mentioned above.

holds for any finite extension L/K and any modulus $\mathfrak{m}$ and can be proved rather easily using analytic techniques.

(2) the Second Inequality says that

$$(D_K\{\mathfrak{f}\} : H_{L/K}\{\mathfrak{f}\}) \geq (L : K),$$

where L/K is a cyclic extension of prime degree l, and where $\mathfrak{f}$ is the conductor of L/K, that is, the ideal such that the relative discriminant of L/K is $\mathfrak{f}^{l-1}$.

In his famous Marburg lectures [30] on class field theory, Hasse puts the proof of the second inequality into historical perspective by mentioning the role of Gauß's work:

> Wir gehen jetzt auf den Beweis des Umkehrsatzes aus. Die dazu erforderlichen Überlegungen des laufenden Paragraphen bilden die Verallgemeinerung der berühmten Gaußschen Untersuchungen über die Theorie der Geschlechter quadratischer Formen aus seinen *disquisitiones arithmeticae*.[42]

In the following, we will provide the background needed for portraying the role of genus theory in the proof of the second inequality of class field theory.

Consider a cyclic extension L/K of prime degree ℓ; then $\operatorname{disc}(L/K) = \mathfrak{f}^{\ell-1}$ for some ideal $\mathfrak{f}$ in $\mathcal{O}_K$ called the conductor of L/K. Takagi's definition of genera in L/K is based on the observation that there is a connection between the class group $\mathrm{Cl}(L)$ and some ray class group Cl_K^ν defined modulo $\mathfrak{f}$: given a class $c = [\mathfrak{A}] \in \mathrm{Cl}(L)$, we can form the ray class $[N_{L/K}\mathfrak{A}]$ in the group Cl_K^ν of ideals modulo norm residues, that is, in the group $D_K\{\mathfrak{f}\}$ of ideals coprime to $\mathfrak{f}$ modulo the group $P_K^\nu\{\mathfrak{f}\}$ of principal ideals generated by norm residues modulo the conductor $\mathfrak{f}$. Note that if $\mathfrak{A} = \lambda\mathfrak{B}$ for some $\lambda \in L^\times$, then the ray classes generated by $N_{L/k}\mathfrak{A}$ and $N_{L/k}\mathfrak{B}$ coincide since $N_{L/K}\lambda \in P_K^\nu\{\mathfrak{f}\}$.

Consider the norm map $N_{L/K} : \mathrm{Cl}(L) \longrightarrow \mathrm{Cl}_K^\nu$. Clearly $\operatorname{im} N = N\,\mathrm{Cl}(L) = H_{L/K}\{\mathfrak{f}\}/P_K^\nu\{\mathfrak{f}\}$, so the image of the norm involves the ideal group associated with L/K. The kernel of the norm map is called the principal genus C_{gen}: it is the group of all ideal classes $c = [\mathfrak{A}] \in \mathrm{Cl}(L)$ such that $N_{L/K}\mathfrak{A} = (\alpha)$ for norm residues $\alpha \in K^\times$ (thus α is coprime to $\mathfrak{f}$ and a norm residue at every prime ideal). Thus we find the following exact sequence

$$1 \longrightarrow C_{\mathrm{gen}} \longrightarrow \mathrm{Cl}(L) \xrightarrow{N} H_{L/K}\{\mathfrak{f}\}/P_K^\nu\{\mathfrak{f}\} \longrightarrow 1. \tag{4}$$

Thus computing the number of genera $g = (\mathrm{Cl}(L) : C_{\mathrm{gen}})$ will help us in getting information about the order of the ideal class group associated to L/K. We will show that $g = a$, where a denotes the number of ambiguous ideal classes in L. In fact, C_{gen} clearly contains the group $\mathrm{Cl}(L)^{1-\sigma}$, where σ is a generator of $\mathrm{Gal}(L/K)$. This shows that

$$a = (\mathrm{Cl}(L) : \mathrm{Cl}(L)^{1-\sigma}) \geq (\mathrm{Cl}(L) : C_{\mathrm{gen}}) = g,$$

[42] We now are going for the proof of the inverse theorem. The considerations of this section, which will be needed to achieve this, are generalizations of Gauß's famous investigations in the genus theory of quadratic forms in his *disquisitiones arithmeticae*.

that is, the first inequality of genus theory. The left hand side can be evaluated explicitly: the ambiguous class number formula says that

$$a = h_K \cdot \frac{\prod e(\mathfrak{p})}{(L:K)(E:E_\nu)},$$

where $h_K = \#\operatorname{Cl}(K)$ is the class number of K, $e(\mathfrak{p})$ is the ramification index of a prime ideal $\mathfrak{p}$ in L/K, the product is over all (ramified) primes in K including the infinite primes, E is the unit group of K, and E_ν its subgroup of units that are norm residues modulo $\mathfrak{f}$.

For proving the second inequality of genus theory, namely $g \ge a$, we use the exact sequence (4) and get

$$(\operatorname{Cl}(L) : C_{\text{gen}}) = (N\operatorname{Cl}(L) : 1) = (H_{L/K}\{\mathfrak{f}\} : P_K^\nu\{\mathfrak{f}\}) = \frac{(D_K\{\mathfrak{f}\} : P_K^\nu\{\mathfrak{f}\})}{(D_K\{\mathfrak{f}\} : H_{L/K}\{\mathfrak{f}\})}.$$

Now the index in the denominator satisfies $(D_K\{\mathfrak{f}\} : H_{L/K}\{\mathfrak{f}\}) \le \ell$ by the first inequality. The index in the numerator is the product of $h_K = (D_K\{\mathfrak{f}\} : P_K\{\mathfrak{f}\})$ (ideals away from $\mathfrak{f}$ modulo the subgroup of principal ideals), that is, the class number of K, and the index $(P_K\{\mathfrak{f}\} : P_K^\nu\{\mathfrak{f}\})$; this last index can be computed explicitly, and it turns out that

$$(P_K\{\mathfrak{f}\} : P_K^\nu\{\mathfrak{f}\}) = (E_\nu : E \cap NL^\times) \cdot \frac{\prod e(\mathfrak{p})}{(E:E_\nu)}.$$

Thus we find

$$(D_K\{\mathfrak{f}\} : P_K^\nu\{\mathfrak{f}\}) = (E_\nu : E \cap NL^\times) \cdot a\ell \ge a\ell;$$

this means that in the sequence of inequalities

$$a \ge (\operatorname{Cl}(L) : C_{\text{gen}}) = g = \frac{(D_K\{\mathfrak{f}\} : P_K^\nu)}{(D_K\{\mathfrak{f}\} : H_{L/K}\{\mathfrak{f}\})} \ge a$$

we must have equality throughout; in particular we find

- $(D_K\{\mathfrak{f}\} : H_{L/K}\{\mathfrak{f}\}) = \ell$: cyclic extensions are class fields;
- The principal genus theorem: $C_{\text{gen}} = \operatorname{Cl}(L)^{1-\sigma}$; note that if L/K is unramified, then $C_{\text{gen}} = \operatorname{Cl}(L)[N]$ coincides with the kernel of the norm map $\operatorname{Cl}(L) \longrightarrow \operatorname{Cl}(K)$, and the principal genus theorem becomes Theorem 1.
- The norm theorem for units: $(E_\nu : E \cap NL^\times) = 1$, that is, any unit that is a norm residue modulo the conductor is the norm of some element of $L^\times$.

Thus the proof of the second inequality consists in a calculation of the number g of genera: the inequality $g \le a$ comes from the ambiguous class number formula, the inequality $g \ge a$ from the first inequality of class field theory and some cohomological results.

Takagi then derives the norm theorem (in cyclic extensions, norm residues modulo the conductor are actual norms) from the principal genus theorem.

Hasse. In his Klassenkörperbericht [28], Hasse reproduces Takagi's proof of the second inequality with only minor modifications. In his Marburg lectures [30], on the other hand, Hasse proves the second inequality

$$(D_K\{\mathfrak{f}\} : H_{L/K}\{\mathfrak{f}\}) \ge (L:K) \tag{5}$$

in a different and direct way; the main advantages of his proof are

- it is valid for cyclic extensions of arbitrary (finite) degree;
- the full norm theorem is a consequence of equality in (5);

- it does not use the first inequality.

This last fact later allowed Chevalley to give an arithmetic proof of class field theory by proving the second inequality first and then deriving the first inequality without analytic means.

At some point in the computation of (5), the index (norm residues modulo conductor : norms) is written as the product of (units that are norm residues : norms of units) and (ideal classes of the principal genus : $(1-\sigma)$-th powers of ideal classes). Thus Hasse's norm theorem (which follows by comparing (5) with the first inequality) contains the principal genus theorem, i.e., the statement that the principal genus consists of the $(1-\sigma)$-th powers of ideal classes.

The General Principal Genus Theorem. Recall that ideal classes in L were mapped by the norm to ray classes modulo $\mathfrak{f}$ in K. Are there similar results connecting ray classes in L with ray classes in K? The answer is yes: in [28, p. 304–310], Hasse proved the 'most general' principal ideal theorem. In order to state it we need the following

Proposition 4. *Let L/K be a cyclic extension of prime degree with generating automorphism σ, and let $\mathfrak{m}$ be a modulus in K. Then there exists a modulus $\mathfrak{M}$ in L such that*

(1) $\mathfrak{M} \mid \mathfrak{m}\mathcal{O}_K$;
(2) $\mathfrak{M}^\sigma = \mathfrak{M}$;
(3) *for $\beta \in L^\times$ coprime to $\mathfrak{M}$ we have $N_{L/K}(\beta) \equiv 1 \bmod \mathfrak{m}$ if and only if $\beta \equiv \alpha^{1-\sigma} \bmod \mathfrak{M}$.*

With these preparations, Hasse defines the principal genus $\overline{H}_1$ mod $\mathfrak{M}$ in L as the group of ray classes modulo $\mathfrak{M}$ whose relative norms land in the ray modulo $\mathfrak{m}$ in K.

Theorem 2. *Let L/K, $\mathfrak{m}$ and $\mathfrak{M}$ be defined as above. Then the principal genus $\overline{H}_1$ coincides with the group of $1-\sigma$-th powers of ray classes mod $\mathfrak{M}$ in L.*

This was generalized even more by Herbrand [34].

12. Chebotarev and Scholz

The generalization of genus theory from cyclic extensions to general normal extensions was mainly the work of Chebotarev [8] and Scholz [67].

Let L/K be a normal extension. The maximal unramified extension of L of the form LF, where F/K is abelian, is called the genus class field L_{gen} of L with respect to K; the maximal unramified extension that is central over K is called the central class field and is denoted by L_{cen}.

According to Scholz, these definitions are due to Chebotarev [8]; as a matter of fact, his paper is not easy reading. The characterization of the genus and central class fields in terms of class groups is due to Scholz:

Theorem 3. *Let L/K be a normal extension of number fields, let H_0 denote the elements of $K^\times$ that are norm residues, and put $N_0 = N_{L/K}L^\times$. Next, let H and N denote the group of ideals in L whose norms land in the groups of principal ideals generated by elements of H_0 and N_0, respectively.*[43] *Then the class field associated*

[43]Observe that H is the principal genus in the sense of Takagi.

to the ideal group H is the genus class field L_{gen}, and the class field associated to N is the central class field L_{cen}. In particular, Scholz's number knot H_0/N_0 is isomorphic to the Galois group of $L_{\text{cen}}/L_{\text{gen}}$.

Scholz used this result to prove that Hasse's norm residue theorem (everywhere local norms are global norms) is valid in all extensions whose Galois groups have trivial Schur multiplier. Jehne [41] presented Scholz's work in a modern language and extended his results.

As an unramified abelian extension of L, L_{gen} corresponds to some quotient $\mathrm{Cl}(K)/C_{\text{gen}}$ of the class group of K, and the group C_{gen} is called the principal genus.

Proposition 5. *If L/K is a cyclic extension, and if σ is a generator of* $\mathrm{Gal}(L/K)$*, then $C_{\text{gen}} = \mathrm{Cl}(L)^{1-\sigma}$.*

The following theorem connects the modern definition of the principal genus with the classical one by Takagi: Fröhlich [21, pp. 18–19] calls it the *classical principal genus theorem*:

Theorem 4. *Let L/K be a cyclic extension, and σ a generator of* $\mathrm{Gal}(L/K)$*. Then $[\mathfrak{a}] \in C_{\text{gen}}$ if and only if $N_{L/K}\mathfrak{a} = (\alpha)$, where $\alpha \in K^\times$ is a norm residue at all ramified primes in L/K.*

This form of genus theory was used by various number theorists; among the many contributions, let us mention Hasse [29] and Leopoldt [52], Gold [26], Stark [79] (whose generalization of genus theory lacks an analogue of Gauß's principal genus theorem), Gurak [27], and Razar [64].

V. Genus Theory and Galois Cohomology

13. Noether

Emmy Noether thought very highly of her version of the principal genus theorem for number fields that she developed in early 1932. It was published in 1933 in a paper [60] which became more famous for the 'Noether equations'[44] in connection with Hilbert's Theorem 90 than for the main content, the principal genus theorem. Expositions of Noether's principal genus theorem can be found in Deuring [10, VII, §7] and Fröhlich [20].

Noether's version. Noether starts with a short introduction to crossed products: let K be a field and L/K a separable extension of degree n and with Galois group G. The crossed product of L and G is an algebra A together with injections $L \hookrightarrow A$ and $G \hookrightarrow A$ such that all automorphisms of L become inner automorphisms of A.

Noether next describes this algebra A using factor systems. As a L-vector space, A is generated by the basis elements $u_{\sigma_1}, \ldots, u_{\sigma_n}$ corresponding to the n group elements s_i; thus we have

$$A = u_{\sigma_1}L \oplus \cdots \oplus u_{\sigma_n}L. \tag{6}$$

[44] Lorenz [53] has observed that these are due to Speiser, and that Noether actually credits him in [60].

The condition that the automorphisms σ on L should become inner can be satisfied by demanding

$$z^\sigma = u_\sigma^{-1} z u_\sigma \tag{7}$$

for every $z \in L$. This defines a factor system $(a_{\sigma,\tau})$ in $L^\times$ by

$$u_\sigma u_\tau = s_{\sigma\tau} a_{\sigma,\tau}, \tag{8}$$

and associativity of multiplication gives the relation

$$a_{\sigma\tau,\rho} a_{\sigma,\tau}^\rho a_{\sigma,\tau\rho} a_{\tau,\rho}. \tag{9}$$

Now the multiplication

$$\sum u_\sigma b_\sigma \cdot \sum u_\tau c_\tau = \sum u_\sigma u_\tau b_\sigma^\tau c_\tau$$

makes A into a simple normal algebra over K which will be denoted by $A = (a_{\sigma,\tau}, L, G)$. Different factor systems $a_{\sigma,\tau}$ and $\overline{a}_{\sigma,\tau}$ generate isomorphic algebras if there are $c_\sigma \in L^\times$ such that

$$\overline{a}_{\sigma,\tau} = a_{\sigma,\tau} c_\sigma^\tau c_\tau / c_{\sigma\tau}. \tag{10}$$

The cosets $u_\sigma L^\times$ define a group extension $G^\times$ of G:

$$1 \longrightarrow L^\times \longrightarrow G^\times \longrightarrow G \longrightarrow 1.$$

The principal genus theorem Noether is about to prove has an analogue for normal extensions, namely Hilbert's Theorem 90: she gives three different formulations of this result.

Proposition 6. *Let L/K be a finite Galois extension with Galois group G. Then the following assertions are equivalent formulations of the 'Minimal' Principal Genus Theorem:*

1. *Every group automorphism of $G^\times$ whose restriction to $L^\times$ is the identity is inner, and is generated by an element of $L^\times$.*
2. *If $c_\sigma^\tau c_\tau / c_{\sigma\tau} = 1$ for all $\sigma, \tau \in G$, then there exists a $b \in L^\times$ such that $c_\sigma = b^{1-\sigma}$ for all $\sigma \in G$.*
3. *The group G has a unique crossed representation class of first degree associated to the trivial factor system.*

Using the language of cohomology groups, the second version of the minimal principal genus theorem claims that $H^1(G, L^\times) = 0$, i.e., it is Hilbert's Satz 90. A representation $u_\sigma \longmapsto C_\sigma$ is called a crossed representation for the factor system $a_{\sigma,\tau}$ if $C_\sigma^\tau C_\tau = C_{\sigma\tau} a_{\sigma,\tau}$. Two crossed representations $u_\sigma \longmapsto C_\sigma$ and $u_\sigma \longmapsto D_\sigma$ for $a_{\sigma,\tau}$ belong to the same class if $C_\sigma = B^{-\sigma} D_\sigma B$.

Noether then defines an *ideal factor system* of a Galois extension L/K with Galois group $\mathrm{Gal}(L/K) = \{\sigma, \tau, \ldots\}$ as a system of n^2 ideals $\mathfrak{a}_{\sigma,\tau}$ of L satisfying the relations

$$\mathfrak{a}_{\sigma,\tau} \mathfrak{a}_{\tau,\rho} = \mathfrak{a}_{\sigma\tau,\rho} \mathfrak{a}_{\sigma,\tau}^\rho.$$

From n ideals $\mathfrak{c}_\sigma$ we can construct a factor system

$$\mathfrak{a}_{\sigma,\tau} = \frac{\mathfrak{c}_\sigma^\tau \mathfrak{c}_\tau}{\mathfrak{c}_{\sigma\tau}}$$

called the transformation system.

Ideal factor systems form a group C, and the transformation systems form a subgroup B of C. In analogy to the group of norm residues modulo the conductor

Noether defines the principal class of ideal factor systems as consisting of systems $\mathfrak{a}_{\sigma,\tau}$ with the following property: there exists a factor system $a_{\sigma,\tau}$ in $L^\times$ such that

(1) $\mathfrak{a}_{\sigma,\tau} = (a_{\sigma,\tau})$;
(2) $a_{\sigma,\tau}$ determines an algebra $\mathfrak{A} = (L, a)$ that splits at every ramified place $\mathfrak{p}$ of L/K.

Then Noether's principal genus theorem states

Theorem 5. *If the transformation system $\mathfrak{c}_\sigma^\tau \mathfrak{c}_\tau \mathfrak{c}_{\sigma\tau}^{-1}$ is in the principal class, then there is an ideal class $[\mathfrak{b}]$ such that $[\mathfrak{c}_\sigma] = [\mathfrak{b}]^{1-\sigma}$ for all $\sigma \in \mathrm{Gal}(L/K)$.*

Noether also gives two formulations analogous to the first and third version of Proposition 6.

Idèles. For stating Noether's principal genus theorem in a modern language we need to introduce the the idèle group J of a number field L, the idèle class group C, the unit idéles U, the group of fractional ideals D and its subgroup P of principal ideals, as well as other well known invariants of L. These groups are all part of the fundamental exact and commutative square

$$\begin{array}{ccccccccc}
 & & 1 & & 1 & & 1 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & E & \longrightarrow & L^\times & \longrightarrow & P & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & U & \longrightarrow & J & \longrightarrow & D & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & \mathcal{E} & \longrightarrow & C & \longrightarrow & \mathrm{Cl} & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 1 & & 1 & & 1 & &
\end{array}$$

Our aim is to reformulate Noether's principal genus theorem in the language of the cohomology of idèles; fix a normal extension L/K of number fields with Galois group $G = \mathrm{Gal}(L/K)$. As all our cohomology groups will be formed with G, we put $H^q(M) := H^q(G, M)$ from now on.

There is a 'Hilbert 90' for idèles: we have $H^1(J_L) = 1$; this is essentially a direct consequence of Hilbert's Theorem 90 for the localizations $L_\mathfrak{p}$. The claim $H^1(C_L) = 1$ is much deeper; in fact, it can be viewed as a generalization of Hasse's norm theorem for cyclic extensions, that is, as a Local-Global Principle for normal extensions.

In order to see this, take the long cohomology sequence of the exact sequence

$$1 \longrightarrow L^\times \longrightarrow J_L \longrightarrow C_L \longrightarrow 1;$$

observing that $H^{-1}(J_L) \simeq H^1(J_L) = 1$ for cyclic groups G we find

$$1 \longrightarrow H^{-1}(C_L) \longrightarrow H^0(L^\times) \xrightarrow{\ i\ } H^0(J_L).$$

Now $H^0(L^\times) = K^\times/N_{L/K}L^\times$, $H^0(J_L) = J_K/NJ_L$, hence $\ker i = \partial_{L/K} := K^\times \cap NJ_L/NL^\times$ is the obstruction to Hasse's Local-Global Principle. Thus $H^1(C) = 1$

is equivalent to Hasse's norm theorem. Observe that $\partial_{L/K} = H_0/N_0$ coincides with Scholz's number knot from Theorem 3.

Roquette's version. Let us now translate Noether's results into the language of cohomology of idèles. We will start with a version due to P. Roquette [66] and then explain how this is connected with A. Fröhlich's 'translation'.

Let $H^2_S(L^\times)$ denote the subgroup of $H^2(L^\times)$ whose elements split at all primes in S; in other words, $H^2_S(L^\times)$ is the kernel of the natural map $H^2(L^\times) \longrightarrow H^2\big(\prod_{w\in S} L_w^\times\big)$ induced by $L^\times \longrightarrow \prod_{w\in S} L_w^\times$ (where $w \in S$ is short for $w \mid v$ for $v \in S$).

Next the exact sequence $1 \longrightarrow E \longrightarrow L^\times \longrightarrow P \longrightarrow 1$ yields a map $H^2_S(L^\times) \longrightarrow H^2(P)$; let H_S denote the image of $H^2_S(L^\times)$ in $H^2(P)$.

Finally, the sequence $1 \longrightarrow P \longrightarrow D \longrightarrow \mathrm{Cl} \longrightarrow 1$ gives us an exact sequence

$$0 = H^1(D) \longrightarrow H^1(\mathrm{Cl}) \xrightarrow{\delta} H^2(P) \xrightarrow{\phi} H^2(D), \tag{11}$$

which allows us to identify $H^1(\mathrm{Cl})$ with a subgroup of $H^2(P)$. In particular, we can talk about $H_S \cap H^1(\mathrm{Cl})$.

Using this language, Noether's principal genus theorem can be stated in the following way:

Theorem 6. *Let L/K be a normal extension of number fields with Galois group G, and let S be the set of ramified primes. Then $H_S \cap H^1(\mathrm{Cl}) = 0$.*

In order to see the conection with Noether's original formulation, observe that a transformation system $\mathfrak{c}_\sigma$ of ideals is a cocycle of the ideal class group and therefore defines an element $c_\sigma \in H^1(\mathrm{Cl})$ if $[\mathfrak{c}_\sigma]^\tau[\mathfrak{c}_\tau] = [\mathfrak{c}_{\sigma\tau}]$ (this is the first condition of the system $\mathfrak{c}_\sigma$ being in the principal class); the claim that $c_\sigma = [\mathfrak{c}_\sigma] = [\mathfrak{b}]^{1-\sigma}$ says that the cocycle is a coboundary, in other words, that $H^1(\mathrm{Cl}) = 1$. This is, however, only true if the second condition is also satisfied; this condition demands that $\mathfrak{c}_\sigma^\tau \mathfrak{c}_\tau \mathfrak{c}_{\sigma\tau}^{-1} = (a_{\sigma,\tau})$ for a factor system $a_{\sigma,\tau} \in H^2(L^\times)$ whose associated algebra splits at every place $\mathfrak{p}$ that is ramified in L/K. In our language, the element $c_\sigma \in H^1(\mathrm{Cl})$ defines a factor set of principal ideals in $H^2(P)$ under the connection homomorphism; if this factor system actually comes from an element in $a_{\sigma,\tau} \in H^2(L^\times)$ whose associated algebra splits at the ramified primes (i.e., if $a_{\sigma,\tau} \in H^2_S(L^\times)$), then Noether's principal genus theorem claims that the element c_σ is trivial.

Proof of Noether's Theorem. Let us now derive Noether's principal genus theorem from class field theory. An ingredient of Noether's proof of the principal genus theorem is what she calls the

Proposition 7 (Principal Genus Theorem for Ideals)**.** *If L/K is a normal extension of number fields with Galois group G, then $H^1(D_L) = 0$, where D_L is the group of fractional ideals in L.*

Our first goal is to prove

Lemma 2. *We have $H^1(C) = 0$ if and only if $H^2_S(L^\times) \longrightarrow H^2(D)$ is injective.*

Proof. Since $H^1(J) = 0$, we find that the Local-Global Principle $H^1(C) = 0$ holds if and only if $H^2(L^\times) \longrightarrow H^2(J)$ is injective.

From the definition of $H_S^2(L^\times)$ and the analogous definition of $H_S^2(J)$ we get the exact and commutative diagram

$$\begin{array}{ccccccc} 0 & \longrightarrow & H_S^2(L^\times) & \longrightarrow & H^2(L^\times) & \longrightarrow & H^2\big(\prod_{w\in S} L_w^\times\big) \\ & & & & \downarrow & & \downarrow \\ 0 & \longrightarrow & H_S^2(J) & \longrightarrow & H^2(J) & \longrightarrow & H^2\big(\prod_{w\in S} L_w^\times\big). \end{array}$$

A simple diagram chase shows that the map $H^2(L^\times) \longrightarrow H^2(J)$ induces a map $H_S^2(L^\times) \longrightarrow H_S^2(J)$, and that $\ker(H^2(L^\times) \longrightarrow H^2(J)) = \ker(H_S^2(L^\times) \longrightarrow H_S^2(J))$.

The natural map $J \longrightarrow D$ from idèles to their ideals induces a homomorphism $H^2(J) \longrightarrow H^2(D)$, so by restriction we get a map $H_S^2(J) \longrightarrow H^2(D)$.

We have already seen that $H^1(C) = 0$ if and only if $H^2(L^\times) \longrightarrow H^2(J)$ is injective, and that $\ker(H^2(L^\times) \longrightarrow H^2(J)) = \ker(H_S^2(L^\times) \longrightarrow H_S^2(J))$.

Thus it remains to show that $H_S^2(J) \longrightarrow H^2(D)$ is injective. The exact sequence $1 \longrightarrow U \longrightarrow J \longrightarrow D \longrightarrow 1$ gives, via the long cohomology sequence, rise to a commutative diagram

$$\begin{array}{ccccccccc} 0 = H^1(D) & \longrightarrow & H^2(U) & \longrightarrow & H^2(J) & \longrightarrow & H^2(D) \\ & & \downarrow & & \downarrow & & \downarrow \\ 0 & \longrightarrow & H^2\big(\prod_{w\in S} L_w^\times\big) & \longrightarrow & H^2\big(\prod_{w\in S} L_w^\times\big) & \longrightarrow & 0. \end{array}$$

Applying the snake lemma gives an exact sequence

$$0 \longrightarrow H_S^2(U) \longrightarrow H_S^2(J) \longrightarrow H^2(D)$$

It remains to show that $H_S^2(U) = 0$ if S contains ramified primes; observe that $U \simeq \prod_{w\in S} U_w \times \prod_{w\notin S} U_w$, hence $H^2(U) \simeq H^2(\prod_{w\in S} U_w) \times H^2(\prod_{w\notin S} U_w)$.

It is known (see e.g. [7, p. 131, Prop. 1.1]) that $H^q(\mathrm{Gal}(L/K), U_L) = 0$ for $q \ge 1$ and unramified extensions L/K of local fields; globally we have $H^q(G, \prod_{w|v} U_w) \simeq H^q(G_{w_0}, U_{w_0})$ by [7, p. 176/177, Prop. 7.2], where w_0 is a fixed prime in L above v, and in particular we have $H^2(U) = H^2(\prod_{w|v\in S} U_w)$, hence $H_S^2(U) = 0$ as claimed.

Thus $\ker(H_S^2(L^\times) \longrightarrow H_S^2(J)) = \ker(H_S^2(L^\times) \longrightarrow H^2(D))$ as claimed □

Now we can prove Noether's Principal Genus Theorem 6:

Proof. Take an element $\delta(c) \in H^1(\mathrm{Cl})$; if $\delta(c) \in H_S$, then there is an element $a \in H_S^2(L^\times)$ such that $\delta(c) = \alpha(a)$, where $\alpha : H_S^2(L^\times) \longrightarrow H^2(P)$. Since (11) is exact, we have $0 = \phi \circ \delta(c) = \phi \circ \alpha(a)$. Since $\phi \circ \alpha$ is injective by assumption, we conclude that $a = 0$, then $0 = \alpha(a) = \delta(c)$ implies $c = 0$ since δ is injective. □

Remark. If L/K is cyclic and if σ generates $\mathrm{Gal}(L/K)$, then $H_S \cap H^1(\mathrm{Cl}) \simeq H_S \cap H^{-1}(\mathrm{Cl})$, where the intersection is taken in $H^0(P)$. We find that H_S is the image of $H_S^0(L^\times)$ in $H^0(P)$, i.e., that H_S is the subgroup of all principal ideals generated by norm residues at the primes in S modulo principal ideals generated by norms.

On the other hand, $H^{-1}(\mathrm{Cl}) = \mathrm{Cl}(L)[\nu]/\mathrm{Cl}(L)^{1-\sigma}$, where $\nu = 1 + \sigma + \ldots + \sigma^{(L:K)-1}$ is the algebraic norm $\nu : \mathrm{Cl}(L) \longrightarrow \mathrm{Cl}(L)$. The image of $H^{-1}(\mathrm{Cl})$ in $H^0(P) = P^G/P^\nu$ under the connecting homomorphism is computed as follows: take $c = [\mathfrak{a}]$ in a class representing an element of $H^{-1}(\mathrm{Cl})$; then $\mathfrak{a}^\nu = (A)$ for some $A \in L^\times$, and clearly $(A)^\sigma = (A)$, so $(A) \in P^G$. The class of c is then mapped to the class of (A).

This means that $H_S \cap H^{-1}(\mathrm{Cl})$ consists of cosets of ideal classes $c \in \mathrm{Cl}(L)$ such that $c = [\mathfrak{a}]$ with $\mathfrak{a}^\nu = (\alpha)$, where $\alpha \in K^\times$ is a local norm at the primes in S. In other words: If L/K is cyclic and S contains the ramified primes, then $H_S \cap H^{-1}(\mathrm{Cl}) = C_{\mathrm{gen}}/\mathrm{Cl}(L)^{1-\sigma}$, and Noether's theorem implies that $C_{\mathrm{gen}} = \mathrm{Cl}(L)^{1-\sigma}$. If L/K is unramified, then we can take $S = \varnothing$ and get back Furtwängler's Theorem 1.

Fröhlich's version. Fröhlich's article [20] contains a cohomological interpretation of Noether's principal genus theorem that differs slightly from Roquette's version above. Here's Fröhlich's account: Let J' denote the ideles that have entries 1 at all places outside of S; then $J' \simeq \prod_{w\in S} L_w^\times$. The projection $J \longrightarrow J'$ and the inclusion $L^\times \longrightarrow J$ give rise to a maps $\pi_1 : H^2(J) \longrightarrow H^2(J')$ and with $\iota : H^2(L^\times) \longrightarrow H^2(J)$; thus $\ker \pi_1 \circ \iota = H_S^2(L^\times)$.

Next he defines maps $\psi : H^2(L^\times) \longrightarrow H^2(P)$ and $\phi : H^2(P) \longrightarrow H^2(D)$ (he uses I instead of D); then $\psi(\ker \pi_1 \circ \iota) = H_S$.

The equivalent of the injectivity of $H_S^2(L^\times) \longrightarrow H^2(D)$ is the statement that $\ker \pi_1 \circ \iota \cap \ker \phi \circ \psi = 0$: in fact, $\ker \pi_1 \circ \iota = H_S^2(L^\times)$ and $\ker \phi \circ \psi = \ker(H^2(L) \longrightarrow H^2(D))$.

Fröhlich's version of Noether's theorem reads:

Theorem 7. *The composition of maps*

$$H^1(\mathrm{Cl}) \longrightarrow H^2(P) \longrightarrow H^2(P)/\psi(\ker \pi_1 \circ \iota)$$

is injective.

In our language: the induced map $H^1(\mathrm{Cl}) \longrightarrow H^2(P)/H_S$ is injective. This is, of course, equivalent to the statement that $H_S \cap H^1(\mathrm{Cl}) = 0$ in $H^2(P)$.

Terada, Tannaka, Deuring. Noether's formulation of the principal genus theorem apparently wasn't very influential, but there have been a few articles picking up her ideas.

Terada [82] stated Hasse's principal genus theorem in the following form: given a cyclic extension L/K, a generator σ of $\mathrm{Gal}(L/K)$, and modules $\mathfrak{m}$ and $\mathfrak{M}$ as in Theorem 2, the following assertions are equivalent:

$$N_{L/K}\mathfrak{A} \equiv 1 \bmod \mathfrak{m} \quad \text{for some ideal } \mathfrak{A} \subseteq \mathcal{O}_L; \tag{12}$$

$$\mathfrak{A} = \mathfrak{B}^{1-\sigma}\alpha \qquad \text{with } \alpha \equiv 1 \bmod \mathfrak{M}. \tag{13}$$

He introduces the crossed homomorphism $\mathfrak{A}_\tau : G \longrightarrow D_L$ by putting $\mathfrak{A}_1 = (1)$, $\mathfrak{A}_\sigma = \mathfrak{A}$, ..., and $\mathfrak{A}_{\sigma^a} = \mathfrak{A}_\sigma^{\sigma^{a-1}}\mathfrak{A}_{\sigma^{a-1}}$ for $0 < a < (L : K)$. Then he observes that (12) is equivalent to the condition

$$\mathfrak{A}_\rho^\tau \mathfrak{A}_\tau \mathfrak{A}_{\rho\tau}^{-1} \equiv 1 \bmod \mathfrak{m} \tag{14}$$

for all $\rho, \tau \in G$, and that (13) is equivalent to the existence of an ideal $\mathfrak{B}$ such that

$$\mathfrak{A}_\rho^\tau = \mathfrak{B}^{1-\sigma}\alpha_\rho, \quad \alpha_\rho \equiv 1 \bmod \mathfrak{M}. \tag{15}$$

These numbers α_ρ satisfy the conditions

$$\alpha_\rho^\tau \alpha_\tau \alpha_{\rho\tau}^{-1} \equiv 1 \bmod \mathfrak{m} \tag{16}$$

for all $\rho, \tau \in G$.

Terada's generalized version of the principal genus theorem then is

Theorem 8. *Let L/K be an abelian extension; then a system $\mathfrak{A}_\rho$ satisfies the condition (14) if and only if there exist an ideal $\mathfrak{B}$ in L and elements $\alpha_\rho \in L^\times$ such that (15) and (16) are satisfied.*

For related results, see Kuniyoshi & Takahashi [46] and Terada [83]. The last result we will mention is a conjecture of Deuring proved by Tannaka [80]:

Theorem 9. *Let L be the Hilbert class field of a number field K. For every ideal $\mathfrak{a}$ in $\mathcal{O}_K$ there is an element $\Theta(\mathfrak{a}) \in L^\times$ with the following properties:*

1. $\mathfrak{a}\mathcal{O}_L = \Theta(\mathfrak{a})\mathcal{O}_L$;
2. *Let $\sigma(\mathfrak{a}) = (\frac{L/K}{\mathfrak{a}})$ be the Artin automorphism, and define the factor set $\varepsilon(\mathfrak{a},\mathfrak{b})$ by*
$$\varepsilon(\mathfrak{a},\mathfrak{b}) = \frac{\Theta(\mathfrak{a})\Theta(\mathfrak{b})^{\sigma(\mathfrak{a})}}{\Theta(\mathfrak{a}\mathfrak{b})}.$$
Then $\varepsilon(\mathfrak{a},\mathfrak{b}) \in E_K$, the unit group of $\mathcal{O}_K$.

From Noether to Gauss

In a letter[45] to Hasse from June 2/3, 1932, Noether writes:

> Im übrigen habe ich anläßlich der Ausarbeitung meines Züricher Vortrags einmal Gauß gelesen. Es wurde behauptet, daß ein halbwegs gebildeter Mathematiker den Gaußschen Hauptgeschlechtssatz kennt, aber nur Ausnahmemenschen den der Klassenkörpertheorie. Ob das stimmt, weiß ich nicht – meine Kenntnisse gingen in umgekehrter Reihenfolge – aber jedenfalls habe ich in bezug auf Auffassung allerhand von Gauß gelernt; vor allem daß es gut ist den Nachweis, daß die durch Faktorensysteme bestimmte Klasseneinteilung eine Strahlkl.-Einteilung ist, an den Schluß zu stellen; der Übergang meiner Fassung zu der Gaußschen geht nämlich unabhängig davon direkt, erst die Spezialisierung auf die Klassenkörpertheorie braucht den Führer. Was ich mache, ist die Verallgemeinerung der Definition der Geschlechter durch Charaktere.[46]

It seems that this letter was written before Noether submitted the final draft of her article: in [60], conductors are not mentioned at all, and the only remarks on ray classes appear at the very beginning of the section on the principal genus theorem. Perhaps her reading of Gauß (and possibly Hasse's response[47]) led to a reformulation of her article.

With this bow of Emmy Noether to Gauß we conclude our survey of the development of the principal genus theorem.

---

[45] See HINT [39].

[46] By the way, during the preparation for my Zurich lecture I read Gauß. It has been claimed that a reasonably educated mathematician knows Gauß's principal genus theorem, but only exceptional people the principal genus theorem of class field theory. I don't know if that's true – in my case it was the other way round – but in any case I learned a lot about perception from Gauß; above all that it is a good idea to place the proof that the classes determined by factor systems are ray classes at the end; the transition from my version to Gauß's can be done independently and directly, only for the specialization to class field theory the conductor is needed. What I am doing is the generalization of the definition of genera using characters.

[47] Almost all of the letters from Hasse to Noether are lost.

Acknowledgements

I would like to thank Peter Roquette for explaining the content of Noether's paper to me, as well as Norbert Schappacher for various helpful comments.

References

[1] A.A. Antropov, *On Euler's partition of forms into genera*, Historia Math. **22** (1995), 188–193 4
[2] A.A. Antropov, *On the history of the concept of genus of binary quadratic form* (Russian), Istor. Metodol. Estestv. Nauk No. **36**, (1989), 17–27 4
[3] A.A. Antropov, *Partitioning of forms by genus and the reciprocity law in L. Euler's work* (Russian), Voprosy Istor. Estestvoznan. i Tekhn. 1989, no. 1, 56–57 4
[4] F. Arndt, *Ueber die Anzahl der Genera der quadratischen Formen*, J. Reine Angew. Math. **56** (1859), 72–78 7, 9
[5] S. Bae, J.K. Koo, *Genus theory for function fields*, J. Austral. Math. Soc. **60** (1996), 301–310 9
[6] D. Buell, *Binary quadratic forms*, Springer-Verlag 1989 2
[7] J.W.S. Cassels, A. Fröhlich, Algebraic Number Fields, Brighton 1965 28
[8] N. Chebotarev, *Zur Gruppentheorie des Klassenkörpers*, J. Reine Angew. Math. **161** (1929), 179–193 23
[9] C. Chevalley, *Review MR 14,729a (*[82]*)*, Math. Reviews (1952) 20
[10] M. Deuring, *Algebren*, Springer-Verlag 1935; Chelsea 1948 7, 24
[11] P.G.L. Dirichlet, *Vorlesungen über Zahlentheorie*, herausgegeben und mit Zusätzen versehen von R. Dedekind; 4th ed. Braunschweig 1893 7
[12] P.G.L. Dirichlet, *Recherches sur diverses applications de l'analyse infinitésimale à la théorie des nombres*, J. Reine Angew. Math. **19** (1839), 324–369; Werke I, 5, 8
[13] P.G.L. Dirichlet, *Recherches sur les formes quadratiques à coéfficients et à indéterminées complexes*, J. Reine Angew. Math. **24** (1842), 291–371; Werke I, 533–619 9
[14] H. Edwards, *Fermat's Last Theorem*, Springer-Verlag 1977; 5th printing 2001 14
[15] L. Euler, *De resolutione formularum quadraticarum indeterminatarum per numeros integros*, Novi. Comm. Acad. Petrop. **9** (1762/62) 1764, 3–33; Opera Omnia I_2, 576–602 4
[16] L. Euler, *De insigni promotione scientiae numerorum*, (E 598), Oct. 26, 1775; Opuscula analytica **2** (1785), 275–314; Opera Omnia I-4, 163–196 3
[17] L. Euler, *Novae demonstrationes circa divisores numerorum formae xx+nyy*, (E 610), Nov. 20, 1775; Nova Acta Acad. Sci. Petropol. **1** (1783), 47–74; Opera Omnia I-4, 197–220 14
[18] L. Euler, C. Goldbach, *Briefwechsel 1729 – 1764*, A.P. Juskevic, E. Winter (eds.), Akademie-Verlag 1965 2
[19] G. Frei, *On the development of the genus of quadratic forms*, Ann. Sci. Math. Quebec **3** (1979), 5–62 2
[20] A. Fröhlich, *Algebraic Number Theory*, in: *Emmy Noether. A tribute to her life and work*, J.W. Brewer, M.K. Smith (eds.), New York - Basel 1981, p. 157–163 24, 29
[21] A. Fröhlich, *Central extensions, Galois groups, and ideal class groups of number fields*, AMS 1983 24
[22] R. Fueter, *Vorwort des Herausgebers*, Euler's Opera Omnia I-4 (1941), VII–XXX 5, 14
[23] Ph. Furtwängler, *Existenzbeweis für den Klassenkörper*, Math. Ann. **63** (1907), 19
[24] P. Furtwängler, *Über das Verhalten der Ideale des Grundkörpers im Klassenkörper*, Monatsh. f. Math. **27** (1916), 1–15 20
[25] C.F. Gauß, *Disquisitiones Arithmeticae*, 1801; French transl. by Poullet Delisle (1807); reprints 1910, 1953; German transl. by H. Maser (1889); English transl. by A.A. Clarke (1965); 2nd rev. ed. Waterhouse et al. (1986); Spanish transl. by H. Barrantes Campos, M. Josephy and Á. Ruiz Zúñiga (1995) 1, 14
[26] R. Gold, *Genera in Abelian extensions*, Proc. Amer. Math. Soc. **47** (1975), 25–28 24

[27] S. J. Gurak, *Ideal-theoretic characterization of the relative genus field*, J. Reine Angew. Math. **296** (1977), 119–124 24
[28] H. Hasse, *Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper. Teil Ia, Beweise zu I.*, Jahresber. DMV **36** (1927), 233–311 1, 22, 23
[29] H. Hasse, *Zur Geschlechtertheorie in quadratischen Zahlkörpern*, J. Math. Soc. Japan **3** (1951), 45–51 24
[30] H. Hasse, *Vorlesungen über Klassenkörpertheorie*, Physica Verlag 1967 7, 21, 22
[31] E. Hecke, *Vorlesungen über die Theorie der algebraischen Zahlen*, Leipzig 1923; reprint Chelsea 1948, 1970; English transl. Springer-Verlag 1981 12
[32] H.E. Heine, *??*, J. Reine Angew. Math. **48** (1854), 254–266 9
[33] Y. Hellegouarch, *Positive definite binary quadratic forms over $k[X]$*, Number Theory, Ulm 1987, 93–119 9
[34] J. Herbrand, *Sur les théorèmes du genre principal et des idéaux principaux*, Abh. Math. Sem. Hamburg **3** (1932), 84–92 23
[35] D. Hilbert, *Über den Dirichletschen biquadratischen Zahlkörper*, Math. Ann. **45** (1894), 309–340 10
[36] D. Hilbert, *Zahlbericht*, DMV 1897; French Transl. 1909/10; reprint 1991; Engl. transl. Springer-Verlag 1998 11, 13, 19
[37] D. Hilbert, *Über die Theorie der relativquadratischen Zahlkörper*, Jahresber. DMV **6** (1899), 88–94 18
[38] D. Hilbert, *Über die Theorie der relativ-Abelschen Zahlkörper*, Acta Math. **26** (1902), 99–132 11
[39] HINT, web page dedicated to the history of number theory at `http://www.rzuser.uni-heidelberg.de/~proquet2/HINT.html` 30
[40] J.W. Hoffman, J. Morales, *Arithmetic of binary cubic forms*, Enseign. Math. (2) **46** (2000), 61–94 2
[41] W. Jehne, *On knots in algebraic number theory*, J. Reine Angew. Math. **311/312** (1979), 215–254 24
[42] B.W. Jones, *The arithmetic theory of quadratic forms*, Wiley 1950 2
[43] L. Kronecker, , Monatsber. Akad. Wiss. Berlin 1864, 285–303 9
[44] T. Kubota, *Remarks on the theorems of Takagi and Furtwängler*, Adv. Stud. Pure Math. **17** (1989), 267–270 20
[45] E.E. Kummer, *Collected papers*, Springer-Verlag 1975 16, 17
[46] H. Kuniyoshi, S. Takahashi, *On the principal genus theorem*, Tohoku Math. J. **5** (1953), 128–131 30
[47] J. L. Lagrange, *Additions aux éléments d'Algèbre d'Euler*; Lyon 1774; Œuvres **7/8** (1973); Engl. Transl. in *Elements of Algebra*, Springer-Verlag 1972; German Transl.: *Lagrange's Zusätze zu Euler's Elementen der Algebra. Unbestimmte Analysis*, Ostwald's Klassiker No. 103, Leipzig 1898 4
[48] T.Y. Lam, *The Algebraic Theory of Quadratic Forms*, Reading 1973; 2nd ed. 1980 2
[49] A.M. Legendre, *Essais sur la théorie des nombres*, 1798; 2nd. ed. 1808; 3rd. ed. 1830 5
[50] F. Lemmermeyer, *Reciprocity Laws. From Euler to Eisenstein*, Springer-Verlag 2000 7
[51] F. Lemmermeyer, *Reciprocity Laws. From Kummer to Hilbert*, in preparation 15
[52] Leopoldt, *Zur Geschlechtertheorie in abelschen Zahlkörpern*, Math. Nachr. **9** (1953), 351–362 24
[53] F. Lorenz, *Ein Scholion zum Satz 90 von Hilbert*, Abh. Math. Sem. Hamburg **68** (1998), 347–362 24
[54] Y. Manin, *Cubic Forms* (Russian), Moscow 1972; Engl. transl. Amsterdam 1986 2
[55] P. Mansion, *Rapport*, Belg. Bull. (3) **30** (1896), 189–193. 7
[56] F. Mertens, *Über die Composition der binären quadratischen Formen*, Sitz.ber. Wien IIa **104** (1895), 103–143 9
[57] F. Mertens, *Ein Beweis des Satzes, dass jede Klasse von ganzzahligen primitiven binären quadratischen Formen des Hauptgeschlechts durch Duplikation entsteht*, J. Reine Angew. Math. **129** (1906), 181–186 9
[58] B. Minnigerode, *Über die Vertheilung der quadratischen Formen mit complexen Coefficienten und Veränderlichen in Geschlechter*, Gött. Nachr. 1873, 160–180 9
[59] T. Nakayama, *Idèle-class factor sets and class field theory*, Annals Math. **55** (1952), 73–84 20

[60] E. Noether, *Der Hauptgeschlechtssatz für relativ-galoissche Zahlkörper*, Math. Ann. **108** (1933), 411–419 24, 30
[61] O'Meara, *Introduction to quadratic forms*, Springer-Verlag 1963; 1973; 2000 2
[62] T. Ono, *A generalization of Gauss's theorem on the genera of quadratic forms*, Proc. Japan Acad. **61** (1985), 109–111 2
[63] T. Pépin, *Composition des formes quadratiques binaires*, Atti Acad. Pont. Nuovi Lincei **33** (1879/80), 6–73 9
[64] M. Razar, *Central and genus class field and the Hasse norm theorem*, Compositio Math. **35** (1977), 281–298 24
[65] H. Reichardt, *Über Dirichlet's zahlentheoretische Arbeiten*, Bericht von der Dirichlet-Tagung, Akademie-Verlag Berlin 1963 8
[66] P. Roquette, *Kommentar zu Emmy Noether's Hauptgeschlechtssatz*, email June 14, 2001 27
[67] A. Scholz, *Totale Normenreste, die keine Normen sind, als Erzeuger nicht-abelscher Körpererweiterungen. 2*, J. Reine Angew. Math. **182** (1940), 217–234 23
[68] J.A. de Séguier, *Formes quadratiques et multiplication complexe*, 1894 9
[69] J.-A. Serret, *Sur les fonctions entières irréductibles suivant un module premier, dans le cas où le degré est une puissance du module*, J. Pures Appl. **18** (1873), 437–451 9
[70] D. Shanks, *Class number, a theory of factorization, and genera*, Proc. Symp. Pure Math. **20** (1970), 415–440 8
[71] D. Shanks, *Gauss's Ternary form reduction and the 2-Sylow subgroup*, Math. Comp. **25** (1971), 837–853 8
[72] J.M. Shyr, *On relative class numbers of certain quadratic extensions*, Bull. Amer. Math. Soc. **81** (1975), 500–502 2
[73] J.M. Shyr, *Class numbers of binary quadratic forms over algebraic number fields*, J. Reine Angew. Math. **307/308** (1979), 353–364 2
[74] Th. Skolem, *Geschlechter und Reziprozitätsgesetze*, Norsk. Math. Forenings Skrifter (1) **18** (1928), 38pp 19
[75] A. Skorobogatov, *Torsors and rational points*, CUP 2001 2
[76] H.J.S. Smith, , Proc. Roy. Soc. London **13** (1864), 278–298; Coll. Math. Papers I, 418–442 9
[77] A. Speiser, *Über die Komposition der binären quadratischen Formen*, in: H. Weber Festschrift (1912), 375–395 9
[78] A. Speiser, *Die Theorie der binären quadratischen Formen mit Koefficienten und Unbestimmten in einem beliebigen Zahlkörper*, Diss. Göttingen 1909 9
[79] H.M. Stark, *The genus theory of number fields*, Comm. Pure Appl. Math. **29** (1976), 805–811 24
[80] T. Tannaka, *A generalized principal ideal theorem and a proof of a conjecture of Deuring*, Ann. Math. **67** (1958), 574–589 30
[81] O. Taussky, *Some non-commutative methods in algebraic number theory*, in: *Emmy Noether in Bryn Mawr* (B. Srinivasan, J. Sally, eds.) (1983), 47–57 13
[82] F. Terada, *On the principal genus theorem concerning the Abelian extensions*, Tohoku Math. J. **4** (1952), 141–152 29, 31
[83] F. Terada, *A note on the principal genus theorem*, Tohoku Math. J. **5** (1953), 211–213 30
[84] C. de la Vallée Poussin, *Recherches arithmétiques sur la composition des formes binaires quadratiques*, Mém. Acad. Belgique **53** (1895/96), mem. no. 3, 59pp. 9
[85] B.A. Venkov, *Elementary Number Theory*, Engl. Transl. 1970 2, 7
[86] H. Weber, *Zahlengruppen in algebraischen Körpern*, Math. Ann. **48** (1897), 433–473
[87] H. Weber, *Zahlengruppen in algebraischen Körpern. II*, Math. Ann. **49** (1898), 83–100
[88] H. Weber, *Lehrbuch der Algebra*, Bd. 3, 1908 11, 12
[89] A. Weil, *Number Theory. An approach through history from Hammurapi to Legendre*, Birkhäuser 1984 5, 7
[90] A. Weil, *On Eisenstein's copy of the Disquisitiones*, Algebraic number theory, 463–469, Adv. Stud. Pure Math. **17**, 1989 7
[91] D. Zagier, *Zetafunktionen und quadratische Körper*, Springer-Verlag 1981 8

CSU San Marcos, Dept. Mathematics, 333 S Twin Oaks Valley Rd, San Marcos, CA 92096-0001, USA

E-mail address: franzl@csusm.edu