

## VIII.3

# The Development of the Principal Genus Theorem

FRANZ LEMMERMEYER

Genus theory today belongs to algebraic number theory and deals with a certain part of the ideal class group of a number field that is more easily accessible than the rest. 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, via Kummer's contributions, all the way to Takagi's reciprocity law for  $p$ -th power residues.

The central theorem in genus theory is the principal genus theorem.<sup>1</sup> Here, we shall outline the development of the principal genus theorem from its conception by Gauss in the context of binary quadratic forms – with hindsight, traces of genus theory can already be found in the work of Euler on quadratic forms and idoneal numbers – to its modern formulation within the framework of class field theory.

Gauss formulated the theorem in the *Disquisitiones Arithmeticae*, but only in passing: after observing in art. 247 that duplicated classes of binary quadratic forms lie in the principal genus, the converse, i.e., the principal genus theorem, is alluded to for the first time in art. 261:

... if therefore all classes of the principal genus can be obtained from the duplication of some class (and the fact that this is always so will be proved in the sequel), ...<sup>2</sup>

The actual statement of the result in art. 286 of the D.A. is then presented in the form of a problem:

1. The name “principal genus theorem” (*Hauptgeschlechtssatz*) was apparently coined by Helmut Hasse in [Hasse 1927], Ia, § 19, pp. 120–128, and then quickly adopted by mathematicians around Emmy Noether.
2. D.A. art. 261: *si itaque omnes classes generis principalis ex duplicatione alicuius classis provenire possunt (quod revera semper locum habere in sequentibus demonstrabitur).*

PROBLEM. Given a binary form  $F = (A, B, C)$  of determinant  $D$  belonging to the principal genus: to find a binary form  $f$  from whose duplication we get the form  $F$ .<sup>3</sup>

This way of presenting the result does not imply any lack of emphasis on Gauss's part. In fact, he wrote about the result and a few of its consequences:

Unless we are strongly mistaken, these theorems have to be counted among the most beautiful in the theory of binary forms, particularly because, despite their extreme simplicity, they are so recondite that their rigorous demonstration cannot be built without the help of so many other investigations.<sup>4</sup>

Gauss's theory of quadratic forms was generalized in several completely different directions: the theory of  $n$ -ary quadratic forms over fields;<sup>5</sup> the arithmetic of algebraic tori;<sup>6</sup> the theory of forms of higher degree,<sup>7</sup> in particular cubic forms;<sup>8</sup> finally the theory of quadratic and, later, general algebraic number fields.

This chapter deals with genus theory of quadratic forms (from Euler to Dirichlet-Dedekind) in sections 1 to 3. From § 4, we shall focus on genus theory of number fields.<sup>9</sup> In this setting, the principal genus theorem for abelian extensions  $k/\mathbf{Q}$  describes the splitting of prime ideals of  $k$  in the genus field  $k_{\text{gen}}$  of  $k$  which, by definition, is the maximal unramified extension of  $k$  that is abelian over  $\mathbf{Q}$ . In § 8 and § 9 below we explain the relationship between genus theory and higher reciprocity laws. The class field theoretic setting will be developed starting in § 10. The paper ends with a discussion of the Galois cohomological connection introduced by Emmy Noether.

---

3. D.A., art. 286. PROBLEMA. *Proposita forma binaria  $F = (A, B, C)$  determinantis  $D$  ad genus principale pertinente: invenire formam binariam  $f$ , e cuius duplicatione illa oriatur.*

4. Our translation of D.A., art. 287: *Haecce theoremata, ni vehementer fallimur, ad pulcherrima in theoria formarum binarium sunt referenda, eo magis quod licet summa simplicitate gaudeant, tamen tam recondita sint ut ipsarum demonstrationem rigorosam absque tot aliarum disquisitionum subsidio condere non liceat.*

5. See for instance [Jones 1950], [Lam 1973], and [O'Meara 1963] for  $n$ -ary forms, and [Buell 1989] for the binary case. A very readable presentation of Gauss's results close to the original is given in [Venkov 1970].

6. See [Shyr 1975], [Shyr 1979] for a presentation of Gauss's theory in this language, and [Ono 1985] for a derivation of the principal genus theorem using results from Shyr's thesis.

7. Recently, Manjul Bhargava developed a theory of composition for a variety of forms. See [Bhargava 2004] and [Belabas 2005].

8. Let us just mention: (i) Eisenstein's results [Eisenstein 1844], cf. the modern treatment in [Hoffman, Morales 2000] via composition of cubic forms à la Kneser; (ii) Manin's viewpoint of obstructions to the local-global principle – see [Manin 1972] and [Skorobogatov 2001].

9. 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 1979].

## 1. Prehistory: Euler, Lagrange, and Legendre

There are hardly any elements of genus theory in the mathematical literature prior to Gauss's *Disquisitiones Arithmeticae*. What one does find, in particular in Leonhard Euler's work, are results and conjectures that would later on be explained by genus theory.

One such conjecture was developed between Christian Goldbach and Leonhard Euler; on March 12, 1753, Goldbach wrote to Euler that if  $p$  is a prime of the form  $4dm + 1$ , then  $p$  can be represented as  $p = da^2 + b^2$ . Euler replied on March 23/April 3:

I have noticed this very theorem quite some time ago, and I am just as convinced of its truth as if I had proof of it.<sup>10</sup>

He then gave the examples

$$\begin{array}{ll} p = 4 \cdot 1m + 1 & \Rightarrow & p = aa + bb \\ p = 4 \cdot 2m + 1 & \Rightarrow & p = 2aa + bb \\ p = 4 \cdot 3m + 1 & \Rightarrow & p = 3aa + bb \\ p = 4 \cdot 5m + 1 & \Rightarrow & p = 5aa + bb \quad \text{etc.} \end{array}$$

and remarked that he could prove the first claim, but not the rest.<sup>11</sup> Euler then went 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.** If  $4n + 1$  is a prime number, and  $d$  is a divisor of this  $n$ , then that number  $4n + 1$  is certainly of the form  $daa + bb$ , if not in integers, then in fractions.<sup>12</sup>

Euler also studied the prime divisors of a given binary quadratic form  $x^2 + ny^2$ ,<sup>13</sup> and observed that those not dividing  $4n$  are contained in half of the possible prime residue classes modulo  $4n$ .<sup>14</sup> Now, as Euler knew and used in his proof of the cubic case of Fermat's Last Theorem, 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

10. See [Euler & Goldbach 1965], Letters 166 and 167: *Ich habe auch eben diesen Satz schon längst bemerkt und bin von der Wahrheit desselben so überzeugt, als wann ich davon eine Demonstration hätte.*

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

12. *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.*

13. In what follows, we shall always talk about proper divisors of quadratic forms, that is, we assume that  $p \mid x^2 + ny^2$  with  $\gcd(x, y) = 1$ .

14. In [Euler 1785], p. 210, this is formulated 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.

for  $n = 5$ . He then saw that the primes  $p \equiv 1, 9 \pmod{20}$  could be represented<sup>15</sup> as  $p = x^2 + 5y^2$  with  $x, y \in \mathbf{N}$ , whereas  $p \equiv 3, 7 \pmod{20}$  could be written as  $2x^2 + 2xy + 3y^2$  with  $x, y \in \mathbf{Z}$ . 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  $D = 5r^2 + 6s^2$ . All of these forms have different classes of divisors.

But as Euler found out,<sup>16</sup> the number  $n = 39$  provides a counterexample because it has "three kinds of divisors":

$$1) \quad D = F, \quad 2) \quad 3D = F, \quad 3) \quad 5D = F.$$

The 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  $D = 5r^2 + 2rs + 8s^2$ . Euler then observed 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  $61 = (\frac{25}{4})^2 + 39(\frac{3}{4})^2$ .

One of the results in which Euler came close to genus theory is related to a conjecture of his that was shown to be false by Joseph-Louis Lagrange; it appears in [Euler 1764]. In his comments on Euler's *Algebra*, Lagrange writes:

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  $4An + r^2 - A$ .<sup>17</sup>

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 was numerical data, even though he also had a proof that  $p = x^2 - ay^2$  implies  $p = 4an + r^2$  or  $p = 4an + r^2 - a$ .<sup>18</sup>

But Euler's conjecture is not correct; Lagrange pointed out the following counterexample: the equation  $x^2 - 79y^2 = 101$  is not solvable in integers, although

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

16. See [Euler 1785], p. 192.

17. See [Lagrange 1774/1877], p. 156–157: *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  $4An + r^2 - A$ .*

18. He wrote  $x = 2at + r$ ,  $y = 2q + s$ , and found that  $p = x^2 - ay^2 = 4am + r^2 - as^2$  for some  $m \in \mathbf{Z}$ . If  $s$  is even, then  $-as^2$  has the form  $4am'$ , and if  $s$  is odd, one finds  $-as^2 = -4am'' - a$ . This proves the claim.

$101 = 4An + r^2 - A$  with  $A = 79$ ,  $n = -4$  and  $r = 38$ . Whether Euler ever heard about Lagrange's counterexample is not clear.

At any rate, the following amendment of conjecture 1 suggests itself, which we shall see below to be equivalent to Gauss's principal genus theorem:

**Conjecture 2.** If  $p$  not dividing  $4a$  is a prime of the form  $4an + r^2$  or  $4an + r^2 - a$ , then one has  $p = x^2 - ay^2$  for rational numbers  $x, y$ .

Historical appraisals of Euler's achievements on this topic range from the wholesale claim that the concept of genera is due to Euler,<sup>19</sup> via a more moderate picture of Euler as a provider of resources for Gauss's theory, all the way to André Weil who called Euler's papers on idoneal numbers "ill coordinated with one another" and complained about the "confused and defective . . . formulations and proofs" in them.<sup>20</sup> Most of all, one must not forget that Euler only had isolated results on (divisors of) numbers represented by quadratic forms, which were subsequently subsumed under a few general theorems (reciprocity, class group, principal genus theorem) of Gauss's theory of quadratic forms.

As is well-known, Joseph-Louis Lagrange introduced reduction and equivalence into the theory of binary quadratic forms. Focusing on which numbers a given form represents, he discovered that an invertible linear change of variables with integer coefficients in the form does not affect the result – he did not fix the sign of the determinant of the transforming substitution, contrarily to Gauss later. In this way he obtained results like the following: *If a prime  $p$  properly divides a number of the form  $x^2 + 5y^2$ , then  $p$  is represented by one of the forms  $x^2 + 5y^2$  or  $2x^2 \pm 2xy + 3y^2$ .* Now, primes represented by  $x^2 + 5y^2$  clearly are congruent to 1, 9 mod 20, those represented by  $2x^2 \pm 2xy + 3y^2$  are 3, 7 mod 20. Lagrange established the converse a little later.<sup>21</sup> Lagrange derived analogous results for forms  $x^2 - ny^2$  and integers  $n$  with  $|n| \leq 12$ , but failed to obtain a general result.

It was left to Adrien-Marie Legendre to complete these investigations by attaching residue classes (actually linear forms such as  $20n + 1$ ,  $20n + 9$ , which he called *diviseurs linéaires*) to Lagrange's equivalence classes of quadratic forms of discriminant  $-4n$  (which he called *diviseurs quadratiques* of  $x^2 - ny^2$ ).<sup>22</sup> Legendre also touched upon the composition of forms and the representation of binary quadratic forms by sums of three squares, a technique that would later reappear, in a more general perspective, in Gauss's D.A. in the proof of the principal genus theorem.<sup>23</sup>

19. See [Antropov 1989a,b], and [Antropov 1995]. However, Euler's usage of the term *genus* is not compatible with Antropov's reading of it.

20. See [Weil 1984], p. 224. For a historical survey of these papers of Euler see [Steinig 1966].

21. The first part of the work alluded to is [Lagrange 1773], the sequel is [Lagrange 1775].

22. See [Legendre 1830], Art. 212, for the 4 *diviseurs quadratiques* of  $x^2 - 39y^2$  and the 6 *diviseurs linéaires* corresponding to each of them. Cf. the later comment in [Dirichlet 1839], p. 424: *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.*

23. See [Weil 1984], p. 313.

TABLE III.

FORMULE.	DIVISEURS	DIVISEURS LINÉAIRES IMPAIRS.
	QUADRATIQUES.	
$t^2 - 39u^2$	$y^2 - 39z^2$	$156x + 1, 25, 49, 61, 121, 133$
	$39z^2 - y^2$	$156x + 23, 35, 95, 107, 131, 155$
	$2y^2 + 2yz - 19z^2$	$156x + 5, 41, 89, 125, 137, 149$
	$19z^2 - 2yz - 2y^2$	$156x + 7, 19, 51, 67, 115, 151$
$t^2 - 41u^2$	$y^2 - 41z^2$	$164x + 1, 5, 9, 21, 23 : 25, 31, 33, 37, 39 : 43, 45, 49, 51, 57 : 59, 61, 73, 77, 81 : 83, 87, 91, 103, 105 : 107, 113, 115, 119, 121 : 125, 127, 131, 133, 139 : 141, 143, 155, 159, 163$
$t^2 - 42u^2$	$y^2 - 42z^2$	$168x + 1, 25, 79, 121, 127, 151$
	$42z^2 - y^2$	$168x + 17, 41, 47, 89, 143, 167$
	$2y^2 - 21z^2$	$168x + 11, 29, 53, 107, 149, 155$
	$21z^2 - 2y^2$	$168x + 13, 19, 61, 115, 159, 157$
$t^2 - 43u^2$	$y^2 - 43z^2$	$172x + 1, 9, 13, 17, 21 : 25, 41, 49, 53, 57 : 81, 97, 101, 109, 117 : 121, 135, 145, 153, 165 : 169$ $172x + 3, 7, 19, 27, 39 : 51, 55, 63, 71, 75 : 91, 115, 119, 123, 131 : 147, 151, 155, 159, 163 : 171$
	$43z^2 - y^2$	
$t^2 - 46u^2$	$y^2 - 46z^2$	$184x + 1, 5, 9, 25, 27 : 55, 41, 49, 59, 73 : 75, 81, 105, 121, 123 : 131, 139, 147, 163, 169 : 177, 179$ $184x + 5, 7, 15, 21, 37 : 45, 53, 61, 63, 79 : 103, 109, 111, 125, 135 : 143, 149, 157, 159, 175 : 181, 183$
	$46z^2 - y^2$	
$t^2 - 47u^2$	$y^2 - 47z^2$	$188x + 1, 9, 17, 21, 25 : 37, 49, 53, 61, 65 : 81, 89, 97, 101, 121 : 145, 149, 153, 157, 165 : 169, 173, 177$ $188x + 11, 15, 19, 25, 31 : 35, 39, 43, 67, 87 : 91, 99, 107, 123, 127 : 135, 139, 151, 163, 167 : 171, 179, 187$
	$47z^2 - y^2$	
$t^2 - 51u^2$	$y^2 - 51z^2$	$204x + 1, 13, 25, 49, 121, 145, 157, 169$
	$51z^2 - y^2$	$204x + 35, 47, 59, 83, 155, 179, 191, 203$
	$3y^2 - 17z^2$	$204x + 7, 31, 79, 91, 139, 163, 175, 199$
	$17z^2 - 3y^2$	$204x + 5, 29, 41, 65, 113, 125, 173, 197$

Fig. VIII.3A. Table of linear and quadratic divisors (extract)  
A.-M. Legendre's *Théorie des nombres*, vol. 1, 1830

## 2. Gauss's *Disquisitiones Arithmeticae*

We briefly recall Gauss's definitions in sec. 5 of the *Disquisitiones*. A binary quadratic form  $F(x, y) = ax^2 + 2bxy + cy^2$  is also denoted by  $(a, b, c)$ . The *determinant* of  $F$  is  $D = b^2 - ac$ . An integer  $n$  is said to be *represented* by  $F$  if 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 art. 229 of the D.A., is the basis for the definition of the genus of a binary quadratic form:

If  $F$  is a primitive form of determinant  $D$ ,  $p$  a prime number dividing  $D$ , 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 all nonresidues.<sup>24</sup>

For  $p = 2$  the claim is correct but trivial. If  $4 \mid D$ , however, then the numbers represented by  $f$  are all  $\equiv 1 \pmod{4}$ , or all  $\equiv 3 \pmod{4}$ . Similarly, if  $8 \mid D$ , the numbers lie in exactly one of the four residue classes  $1, 3, 5$  or  $7 \pmod{8}$ . For odd primes *not* dividing the discriminant, Gauss observes in the same art. 229:

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  $D$ .<sup>25</sup>

The only exception occurs for the residue classes modulo 4 and 8 of representable odd numbers in the case where  $D$  is odd:

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

Gauss uses these observations in D.A., art. 230, to define the (*total*) *character* of a primitive binary quadratic form. For example, to the quadratic form  $(7, 0, 23)$  of determinant  $-7 \cdot 23 = -161 \equiv 3 \pmod{4}$  he attaches the total character  $1, 4; R7; N23$  because the integers represented by  $7x^2 + 23y^2$  are  $\equiv 1 \pmod{4}$ , quadratic residues modulo 7, and quadratic nonresidues modulo 23. Gauss observes that if  $(a, b, c)$  is a primitive quadratic form, then a prime  $p$  dividing  $b^2 - ac$  does not divide  $\gcd(a, c)$ , 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

- 
24. Our translation of D.A., art. 229: *THEOREMA. Si F forma primitiva determinantis D, p numerus primus ipsum D metiens: tum numeri per p non divisibiles qui per formam F repraesentari possunt in eo convenient, ut vel omnes sint residua quadratica ipsius p, vel omnes non residua.*
  25. D.A., art. 229: *Ceterum, si ad propositum praesens necessarium esset, facile demonstrare possemus, numeros per formam F repraesentabiles ad nullum numerum primum qui ipsum D non metiatur, talem relationem fixam habere, sed promiscue tum residua tum non-residua numeri cuiusvis primi ipsum D non metientis per formam F repraesentari posse.*

in the same class have the same total character, so the notion of character passes to classes of forms. A *genus*<sup>26</sup> of quadratic forms is then defined to consist of all classes with the same total character. The *principal genus* is the genus containing the principal class, i.e., the class containing the form  $(1, 0, -D)$  of determinant  $D$ .

In art. 261 of the D.A., Gauss proves the *first inequality* of genus theory: at least half of all possible total characters do not occur. In art. 262, the quadratic reciprocity law is deduced from this first inequality.

After having studied the representations of binary quadratic forms by ternary forms, Gauss returns to binary quadratic forms in art. 286, and now proves the principal genus theorem quoted in our introduction. This immediately implies the *second inequality* of genus theory in art. 287: at least half of all possible total characters do in fact occur. Finally, in art. 303, Gauss characterizes Euler's idoneal numbers using genus theory. One of the key ingredients of genus theory is the determination of the number of the so-called *ambiguous classes*<sup>27</sup> in arts. 257–259 of the D.A.

A word on terminology may be in order: In his 1932–1933 Marburg lectures on Class Field Theory, Helmut Hasse wrote: “The term *ambig*, whose usage in this connection is somewhat unfortunate, is due to Gauss.”<sup>28</sup> Gauss, however, had of course written in Latin and called an “ambiguous” quadratic form *forma anceps*. From Dedekind we learn:

When giving 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 editions (1871, 1879), ... I called them *ambige Formen* following Kummer, who used this notation in a related area.<sup>29</sup>

26. This terminology, which fits in with the *orders* and *classes* of quadratic forms that Gauss defines in arts. 234–256 of the D.A., is obviously inspired by biology. Carl von Linné (1707–1778) had classified the living organisms into kingdoms (plants, animals), classes, orders, genera, and species. Ernst Eduard Kummer would use the German *Gattung* for Gauss's latin *genus*, but in the long run the translation *Geschlecht* prevailed in Germany.

27. Gauss called a class of forms *anceps* if it was “opposite to itself” (D.A., art. 224: *classes sibi ipsis oppositae*), in other words, if its order in the class group divides 2.

28. See [Hasse 1967], p. 158: *Die in diesem Zusammenhang nicht sehr glückliche Bezeichnung “ambig” stammt von Gauss*. Hasse apparently worked from Maser's German translation of the D.A. which does have *ambig*. Clarke in his English translation of the D.A. used “ambiguous,” whereas I. Adamson used “ambig” in his English translation of Hilbert's *Zahlbericht*.

29. See [Dirichlet 1863/1894], p. 139: *Im mündlichen Vortrage gebrauchte Dirichlet immer die Bezeichnung forma anceps, welche ich auch bei der Ausarbeitung der ersten Auflage (1863) beibehalten habe; in der zweiten und dritten Auflage (1871, 1879), wo diese Formen und die ihnen entsprechenden Formen-Classen häufiger auftraten (§§ 152, 153), habe ich sie im Anschluss an die von Kummer (Monatsber. d. Berliner Akad. vom 18. Februar 1858) auf einem verwandten Gebiete benutzte Bezeichnung ambige Formen genannt*. As a matter of fact, A.C.M. Poulet-Delisle in his 1807 French translation of the D.A., already used *classe ambiguë*; Kummer may have got his term from there.

In the fourth edition (1894), Dedekind replaced *ambig* by “twosided” (*zweiseitig*), i.e., the German translation of *anceps*.

Gauss used his theory of *ternary quadratic forms* to prove the principal genus theorem, but also to derive Legendre’s theorem,<sup>30</sup> as well as the celebrated 3-squares theorem to the effect that every positive integer not of the form  $4^a(8b + 7)$  can be written as a sum of three squares. Friedrich Arndt first, and later Dedekind and Paul Mansion<sup>31</sup> realized that Legendre’s theorem is sufficient for proving the principal genus theorem. This simplified genus theory considerably<sup>32</sup> – see [Lemmermeyer 2000], chap. 2.<sup>33</sup>

### 3. Dirichlet and Dedekind

Johann Peter Gustav Lejeune-Dirichlet is said<sup>34</sup> to have never put Gauss’s *Disquisitiones Arithmeticae* on the bookshelf, but to have always kept the copy on his desk and taken it along even on journeys. He is well-known for having simplified Gauss’s exposition (sometimes by restricting to a special case), thereby making the D.A. accessible to a wider circle of mathematicians. In [Dirichlet 1839], he replaced Gauss’s notation  $aRp, aNp$  for quadratic (non)residues by Legendre’s symbol  $\left(\frac{a}{p}\right) = \pm 1$ , thus giving Gauss’s characters the now familiar look. But his main contribution in this paper was an analytic proof of the second inequality of genus theory.<sup>35</sup>

Dirichlet’s results were added as supplement IV and X of Dedekind’s edition of Dirichlet’s Lectures. Thus in § 122 of [Dirichlet 1863/1894] an integer  $\lambda$  is defined by

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

and in § 123 the first inequality of genus theory is proved:  $g \leq 2^{\lambda-1}$ . In § 125, Dedekind gives Dirichlet’s analytic proof of the existence of these genera, i.e., the

30. To the effect that the equation  $ax^2 + by^2 + cz^2 = 0$  has a nontrivial solution in integers if and only if the coefficients do not have the same sign, and  $-bc$ ,  $-ca$ , and  $-ab$  are squares modulo  $a$ ,  $b$ , and  $c$ , respectively.

31. See [Arndt 1859], [Dirichlet 1863/1894], and [Mansion 1896].

32. Note, however, that Gauss’s proof was constructive, while those based on Legendre’s theorem are not.

33. Legendre’s theorem does not seem to imply the 3-squares theorem. In [Deuring 1935], VII, § 9, a beautiful proof is sketched which uses the theory of quaternion algebras – see also [Weil 1984], III, App. II, pp. 292–294. In 1927, Venkov used Gauss’s theory of ternary quadratic forms to give an arithmetic proof of Dirichlet’s class number formula for negative discriminants  $-m$  in which  $m$  is the sum of three squares – see [Venkov 1970]. Shanks [Shanks 1971a] used binary quadratic forms to develop his clever factorization algorithm SQUFOF (short for SQUare FORM Factorization) and Gauss’s theory of ternary quadratic forms for an algorithm to compute the 2-class group of complex quadratic number fields – see [Shanks 1971b].

34. See [Reichardt 1963], p. 14. [Editors’ note: see also chaps. I.1 and II.2 above].

35. Cf. [Zagier 1981] for a modern exposition of it.

second inequality of genus theory:

The number of existing genera is  $2^{2-1}$ , and all these genera contain equally many classes of forms.<sup>36</sup>

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

Dedekind returned to the 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 adds:

It is impossible for us to go here into communicating 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 abstain from deriving this result without the use of Dirichlet's principles, in a second way, which will at the same time form the basis for other important investigations.<sup>37</sup>

This new 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  $2D$ .<sup>38</sup>

In § 158, Dedekind gives a proof of the principal genus theorem based on Legendre's theorem, referring to [Arndt 1859] for a first proof of this kind.

#### 4. David Hilbert

Although Dedekind introduced ideals and maximal orders in number fields, he did not translate genus theory into his new language. David Hilbert on the other hand worked on the arithmetic of quadratic extensions of  $\mathbf{Q}(i)$  even before his report on algebraic number fields [Hilbert 1897]. His goal then was to

extend 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,

36. See [Dirichlet 1863/1871], p. 324: *Die Anzahl der wirklich existierenden Geschlechter ist gleich  $2^{2-1}$ , und alle diese Geschlechter enthalten gleich viele Formenklassen.*

37. See [Dirichlet 1863/1871], p. 407: *Wir können hier unmöglich darauf eingehen, den Beweis mitzuthellen, 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 Principien auf einem zweiten Wege abzuleiten, der zugleich die Grundlage für andere wichtige Untersuchungen bildet.*

38. See [Dirichlet 1863/1894], § 155, p. 408: *Ist  $(A, B, C)$  eine Form des Hauptgeschlechtes der Determinante  $D$ , so ist die Gleichung  $Az^2 + 2Bzy + Cy^2 = x^2$  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.<sup>39</sup>

Let  $\mathbf{Z}[i]$  denote the ring of Gaussian integers, and let  $\delta \in \mathbf{Z}[i]$  be a squarefree nonsquare. Hilbert considers the quadratic extension  $K = \mathbf{Q}(\sqrt{\delta})$  of  $k = \mathbf{Q}(i)$ , computes integral bases, and determines the decomposition of primes. For the definition of the genus, Hilbert then introduces the prototype of his norm residue symbol. For  $\sigma \in k$  and  $\lambda$  a prime divisor different from  $(1+i)$  of the discriminant of  $K/k$ , Hilbert writes  $\sigma = \alpha\nu$  as a product of a relative norm  $\nu$  and some  $\alpha \in \mathbf{Z}[i]$  not divisible by  $\lambda$ , and puts

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

where  $[\cdot]$  is the quadratic residue symbol in  $\mathbf{Z}[i]$ . (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

$$\left[ \frac{\sigma}{\lambda_1 : \delta} \right], \dots, \left[ \frac{\sigma}{\lambda_s : \delta} \right],$$

where  $\lambda_1, \dots, \lambda_s$  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 then formulated thus:

Each ideal class in the principal genus is the square of some ideal class.<sup>40</sup>

Hilbert went on to determine the number of genera, derived the quadratic reciprocity law, and finally gave an arithmetic proof of the class number formula for  $\mathbf{Q}(i, \sqrt{m})$  and  $m \in \mathbf{Z}$ . He apparently had not yet realized that his symbols  $\left[ \frac{\sigma}{\lambda : \delta} \right]$  were norm residue symbols, nor that the quadratic reciprocity law could be expressed via a product formula for them.

He took these steps in the third section of his *Zahlbericht* [Hilbert 1897] dealing with the theory of quadratic number fields. There he called an integer  $n$  a norm residue<sup>41</sup> at  $p$  in  $\mathbf{Q}(\sqrt{m})$  if  $m$  is a square or if for all  $k \geq 1$  there exist integers  $x, y \in \mathbf{Z}$  such that  $n \equiv x^2 - my^2 \pmod{p^k}$ .

39. The complete quotation from the introduction of [Hilbert 1894] 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.*

40. See [Hilbert 1894], § 4: *Eine jede Idealklasse des Hauptgeschlechtes ist gleich dem Quadrat einer Idealklasse.*

41. I will adopt 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 every power  $\mathfrak{p}^k$ .

Then he defined the norm residue symbol by

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

Hilbert used the norm residue symbol to define characters on ideal classes and defined the principal genus to consist of those ideal classes with trivial character system. In [Hilbert 1897], § 68, he employed ambiguous ideals and his famous *Satz 90* to prove that quadratic number fields with exactly one ramified prime have odd class number. The quadratic reciprocity law is deduced from this in § 69, and the version for quadratic number fields of the principal genus theorem in § 72, including an acknowledgement of the *Disquisitiones Arithmeticae*:

In a quadratic number field, each class of the principal genus is the square of a class [GAUSS (1)].<sup>42</sup>

Hilbert's proof uses a reduction technique reminiscent of Lagrange; the solvability of the norm equation  $n = x^2 - my^2$  for  $x, y \in \mathbf{Q}$  is equivalent to the fact that the ternary quadratic form  $x^2 - my^2 - nz^2$  nontrivially represents 0 in integers. Hilbert explicitly referred to Lagrange when he stated :

If  $n, m$  denote two rational integers, of which  $m$  is not a square, and which for any prime  $w$  satisfy the condition  $\left(\frac{n, m}{w}\right) = +1$ , then  $n$  is the norm of an integral or fractional number  $\alpha$  of the field  $k(\sqrt{m})$ .<sup>43</sup>

Note in passing that this is a special case of Hasse's Norm Theorem, according to which elements that are local norms everywhere (with respect to a cyclic extension) are global norms. The ambiguous class number formula (*Satz 108*, § 77) follows, and finally Hilbert gives a second proof of the principal genus theorem using Dirichlet's analytic techniques, in § 82.

With Hilbert's 1897 *Zahlbericht*, the translation of Gauss's genus theory of binary quadratic forms into the corresponding theory of quadratic extensions was complete. Distinctive features of Hilbert's presentation are the central role of the ambiguous class number formula, the introduction of norm residue symbols, and the corresponding formulation of the reciprocity law as a product formula. Although Hilbert saw that the norm residue symbol for the infinite rational prime<sup>44</sup> would simplify the presentation, he chose not to use it. But these symbols could no longer be avoided when he replaced the rational numbers by arbitrary base fields  $k$  in his article [Hilbert 1898] on class field theory in the quadratic case.

42. [Hilbert 1897], § 71, *Satz 103*: *In einem quadratischen Körper ist jede Klasse des Hauptgeschlechts stets gleich dem Quadrat einer Klasse* [GAUSS (1)].

43. [Hilbert 1897], § 71, *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  $\alpha$  des Körpers  $k(\sqrt{m})$ .* Here  $k(\sqrt{m})$  denotes the quadratic number field  $k$  one gets by adjoining  $\sqrt{m}$  to the field of rational numbers.

44. See [Hilbert 1897], § 70; Hilbert wrote it as  $\left(\frac{n, m}{-1}\right)$ .

## 5. Heinrich Weber

In the third volume of his algebra [Weber 1908], § 108, Heinrich Weber gave an account of genus theory that shows Hilbert's influence: Even though Weber did not include the theory of the quadratic Hilbert symbol, he did realize the importance of the concept of norm residues.

For a modulus  $m \in \mathbf{N}$  and a natural number  $S$  divisible by  $m$ , Weber formed the multiplicative group  $Z$  of rational numbers  $\frac{a}{b}$  relatively prime to  $S$ , that is,  $a, b \in \mathbf{Z}$  and  $\gcd(a, S) = \gcd(b, S) = 1$ . The kernel of the natural map  $Z \rightarrow (\mathbf{Z}/m\mathbf{Z})^\times$  is the group  $M$  of all elements of  $Z$  that are congruent to 1 mod  $m$ , and Weber observed that  $(Z : M) = \phi(m)$ .

Now let  $\mathcal{O}$  denote an order of a quadratic number field  $k$  (Weber wrote  $\mathcal{Q}$  instead of  $\mathcal{O}$ ) such that the prime factors of the conductor of  $\mathcal{O}$  divide  $S$ ; in particular, the discriminant  $\Delta$  of  $\mathcal{O}$  is only divisible by primes dividing  $S$ . The set of integers  $a \in \mathbf{Z}$  for which there is an  $\omega \in \mathcal{O}$  with  $N\omega \equiv a \pmod{m}$  form a subgroup  $A$  of  $Z$  containing  $M$ , namely, the group of norm residues modulo  $m$  of  $\mathcal{O}$ . To simplify the presentation, let  $A\{m\}$  denote this group of norm residues modulo  $m$ . Weber in [Weber 1908], § 107, observed that if  $m = m_1 m_2$  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 the following section § 108, he proved that

$$(Z : A\{p^t\}) = \begin{cases} 1 & \text{if } p \text{ does not divide } \Delta \\ 2 & \text{if } p \text{ divides } \Delta \end{cases}$$

for an odd prime  $p$ , and

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

If  $r$  is a norm residue modulo  $m$  for any modulus  $m$  prime to  $r$ , Weber called  $r$  an *absolute norm residue*; the set of all such  $r \in Z$  forms a group  $R$ .<sup>45</sup> As a consequence of his index computations above, Weber obtained  $(Z : R) = 2^\lambda$ , where  $\lambda$  is the number of *discriminant divisors* of  $\Delta$ . Here a divisor  $\delta$  of  $\Delta$  is called a *discriminant divisor* if both  $\delta$  and  $\Delta/\delta$  are discriminants.

In [Weber 1908], § 109, the genus of an ideal is defined to be the set of all ideals  $a$  coprime to  $\Delta$  whose norms  $Na$  are in the same coset of  $Z/R$ . Weber observes that equivalent ideals have the same genus. The principal genus is the group of all ideals relatively prime to  $\Delta$  such that  $Na \in R$ . He shows that the existence of primes that are quadratic nonresidues modulo  $\Delta$  implies that the number  $g$  of genera satisfies the inequality  $g \leq \frac{1}{2}(Z : R)$ , and that the existence of such primes is equivalent to the quadratic reciprocity law. The fact that this inequality is in fact an equality is proved in § 113 of [Weber 1908] with the help of Dirichlet's analytic methods.

The local nature of the index calculations is much more visible in Weber's treatment than in Hilbert's. Weber's index formulas are closely related to Gauss's observation in the second passage from art. 229 of the D.A. quoted in § 2 above.

45. See [Weber 1908], §§ 108–109.

## 6. Erich Hecke

Erich Hecke's *Vorlesungen über die Theorie der algebraischen Zahlen* [Hecke 1923] contains a masterful exposition of algebraic number theory including the genus theory of (the maximal orders of) quadratic fields. Shortly after the publication of this textbook, during the reformulation of class field theory in the 1930s, genus theory would be thrust into the background, as local methods gradually replaced it in the foundation of class field theory.

Hecke's presentation of genus theory in quadratic fields  $k$  with discriminant  $d$  combined known features with novel ones. First, Hecke used class groups in the strict sense. Already Hilbert had seen that this simplified the exposition of genus theory because some of the statements "can be expressed in a simpler way by using the new notions."<sup>46</sup> Second, Hecke used Weber's index computation for norm residues, but restricted his attention right from the start to norm residues modulo  $d$ . Third, Hecke gave 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 finally obtained the following characterizations:<sup>47</sup>

**Proposition.** 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)  $\left(\frac{N\mathfrak{a}, d}{p}\right) = +1$  for all primes  $p \mid d$ .
- (3)  $N\mathfrak{a} = N(\alpha)$  for some  $\alpha \in k^\times$ .
- (4)  $N\mathfrak{a} \equiv N(\alpha) \pmod{d}$  for some  $\alpha \in k^\times$ .

Hecke, not surprisingly, proved the existence of genera analytically:

The fact that the number  $g$  of genera is  $= 2^{t-1}$  can be proved most conveniently by using transcendental methods.<sup>48</sup>

After the statement of his *Fundamentalsatz über die Geschlechter*, Hecke remarks that "Gauss was the first to discover this theorem and gave a purely arithmetic proof of it."<sup>49</sup>

46. See [Hilbert 1897], § 83–84. The quote is from the end of §84: ... und einige [dieser Tatsachen] erhalten bei Verwendung der neuen Begriffe sogar noch einen einfacheren Ausdruck.

47. This result summarizes parts of Theorems 138–141 and 145 in [Hecke 1923].

48. See [Hecke 1923], § 48, paragraph preceding Satz 144: Die Tatsache, daß die Anzahl der Geschlechter  $g$  genau  $= 2^{t-1}$  ist, wird nun am bequemsten mit Benutzung transzendenter Methoden ... bewiesen.

49. See [Hecke 1923], § 48, remark following Satz 145: Gauss hat diesen Satz zuerst gefunden und für ihn einen rein arithmetischen Beweis gegeben.

## 7. Euler's Conjecture Revisited

In this section we will show that the modified Euler Conjecture 2 of § 1 above follows from genus theory. Assume that  $n$  is a positive squarefree integer and that  $p \equiv 1 \pmod{4n}$  is prime. Then  $\left(\frac{p}{p_i}\right) = +1$  for all primes  $p_i \mid n$ , which by quadratic reciprocity implies  $\left(\frac{d_i}{p}\right) = \left(\frac{p_i}{p}\right) = +1$ , where  $d_i$  are the prime discriminants<sup>50</sup> dividing the discriminant  $d$  of  $\mathbf{Q}(\sqrt{n})$ . Applying the following proposition with  $a = -n$  then proves the Goldbach-Euler conjecture for squarefree  $n$ :

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

- (i) there exist  $x, y \in \mathbf{Q}$  with  $p = x^2 - ay^2$ ;
- (ii) we have  $\left(\frac{d_i}{p}\right) = 1$  for all prime discriminants  $d_i$  dividing the discriminant of  $k$ ;
- (iii) we have  $p\mathcal{O}_k = \mathfrak{p}\mathfrak{p}'$ , and  $\mathfrak{p}$  is equivalent (in the strict sense) to the square of an ideal in  $\mathcal{O}_k$ .

**Proof.** Condition (i) says that the norm of a prime ideal  $\mathfrak{p}$  above  $p$  is the norm of an element, which by Hecke's Proposition (see § 6 above) implies that  $\mathfrak{p}$  is in the principal genus, i.e., (iii). Similarly, if  $p$  does not divide  $d$ , then the Legendre symbols  $\left(\frac{d_i}{p}\right)$  essentially coincide with the Hilbert symbols  $\left(\frac{p_i d}{p_i}\right)$ , where  $p_i$  is the unique prime dividing  $d_i$ , and this time we see that  $\mathfrak{p}$  is in the principal genus by part (2) of Hecke's Proposition. Finally, (iii)  $\Rightarrow$  (i) is proved by taking norms.

Looking at Lagrange's counterexample to Euler's original conjecture in the light of Hecke's genus theory, observe that 79 is the smallest natural number  $a$  such that the class group of  $\mathbf{Q}(\sqrt{a})$  is strictly larger than the genus class group.

The above proposition shows in fact the *equivalence* of the amended Conjecture 2 of § 1 with the Principal Genus Theorem, in view of the following observation whose proof is a simple exercise using the quadratic reciprocity law:

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

- 1. There exist  $n, r \in \mathbf{Z}$  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  $d$ .

To the best of my knowledge, this equivalence has never been noticed before.<sup>51</sup> In his preface to Euler's *Opera Omnia*, Karl Rudolf Fueter remarks<sup>52</sup> that Euler's observation in [Euler 1775] to the effect 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 himself had remarked in art. 151 of the D.A. that there was a gap in Euler's proof. H.M. Edwards has observed:

50. A prime discriminant is a discriminant of a quadratic number field that is a prime power.

51. Not by Lagrange (who disproved Euler's conjecture), nor by Legendre (who proved a result on  $ax^2 + by^2 + cz^2$ , which contains criteria for the solvability of  $-c = aX^2 + bY^2$  in rational numbers as a special case), nor apparently anywhere else in the literature.

52. See [Fueter 1941], p. xiii.

“The case  $D = 79$  is one that Gauss frequently uses as an example,”<sup>53</sup> and has gone on to suggest that Gauss’s interest in this discriminant may have been sparked by Lagrange’s counterexample to Euler’s conjecture.

### 8. Ernst Eduard Kummer

Kummer’s motivation for creating a genus theory for Kummer extensions over  $\mathbf{Q}(\zeta)$ , where  $\zeta$  is a primitive  $\ell$ -th root of unity and  $\ell$  an odd prime number, was his quest for a proof of the reciprocity law for  $\ell$ -th powers: call an  $\alpha \in \mathbf{Z}[\zeta]$  *primary* if  $\alpha$  is congruent to a nonzero integer modulo  $(1 - \zeta)^2$  and if  $\alpha\bar{\alpha}$  is congruent to an integer modulo  $\ell$ . Given two primary, coprime integers  $\alpha, \beta \in \mathbf{Z}[\zeta]$ , Kummer had conjectured the reciprocity law  $\left(\frac{\alpha}{\beta}\right) = \left(\frac{\beta}{\alpha}\right)$  for the  $\ell$ -th power residue symbol. When all other methods of proof had failed (in particular cyclotomic methods via Gauss and Jacobi sums), he turned to Gauss’s genus theory.

Let us write  $\lambda = 1 - \zeta$ , and  $\mathfrak{l} = (\lambda)$  for the prime ideal<sup>54</sup> in  $k = \mathbf{Q}(\zeta)$  above  $\ell$ . Let  $M$  denote the set of all  $\alpha \in k^\times$  coprime to  $\mathfrak{l}$ . Assume that  $\alpha \in \mathbf{Z}[\zeta]$  satisfies  $\alpha \equiv 1 \pmod{\lambda}$ , and write it as  $\alpha = f(\zeta)$  for some polynomial  $f \in \mathbf{Z}[X]$ ; evaluate the  $r$ -th derivative of  $\log f(e^v)$  with respect to  $v$  at  $v = 0$ , and call the result  $\mathcal{L}^r(\alpha)$ .<sup>55</sup> For  $1 \leq r \leq \ell - 2$ , the resulting integer modulo  $\ell$  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  $r = \ell - 1$ . We will not follow here Kummer’s *tour de force* to set up his formalism, but only give the conclusion.<sup>56</sup>

Put  $K = \mathbf{Q}(\zeta_\ell)$ , fix an integer  $\mu \in \mathbf{Z}[\zeta_\ell]$  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  $\mathcal{O} = \mathbf{Z}[\zeta_\ell]$ ; observe that  $\mathcal{O}[w] \neq \mathcal{O}_L$  in general even when  $\mu$  is squarefree. He introduced 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 observed that  $\ell\mathcal{O}[w] \subseteq \mathcal{O}_z \subseteq \mathcal{O}[w]$ . Assume that  $\mathfrak{p}$  is a prime ideal in  $\mathbf{Z}[\zeta]$  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  $\pi$  in general. But not always: since it turns out that  $\mathcal{L}^{2r+1}(\varepsilon_j) = 0$  for all real units  $\varepsilon_j$  and all  $0 \leq r \leq \rho = \frac{1}{2}(\ell - 1)$ , and since moreover  $\mathcal{L}^{2r+1}(\zeta) = 0$  for all  $1 \leq r \leq \rho$ , the quantity  $\mathcal{L}^{2r+1}(\mathfrak{p}) = \frac{1}{h}\mathcal{L}^{2r+1}(\pi)$  is well defined.

This allowed Kummer to define characters  $\chi_3, \chi_5, \dots, \chi_{\ell-2}$  on the group of ideals in  $\mathcal{O}_z$  which are prime to  $\ell \cdot \text{disc}(L/K)$  by putting

$$\chi_{2r+1}(\mathfrak{P}) = \zeta^{\mathcal{L}^{2r+1}(N_{L/K}\mathfrak{P})}, \quad \text{to which he added} \quad \chi_{\ell-1}(\mathfrak{P}) = \zeta^{\frac{1-N\mathfrak{P}}{\ell}}.$$

53. See [Edwards 1977], p. 274; Edwards explicitly mentions D.A., arts. 185, 186, 187, 195, 196, 198, 205, 223 as examples.

54. For Kummer: the “ideal prime number.”

55. Kummer wrote  $\frac{d_v^r \log f(e^v)}{dv^r}$  instead.

56. Kummer’s work on reciprocity laws is spread out over several papers; the main articles are [Kummer 1850], [Kummer 1859], and [Kummer 1861]. As noticed by Takagi and Hasse, Kummer’s differential logarithms can be neatly described algebraically. A detailed exposition will be given in the forthcoming [Lemmermeyer 2007].

Now let  $\mathfrak{p}_1, \dots, \mathfrak{p}_t$  denote the primes different from  $(\lambda)$  that are ramified in  $L/K$ . For each such prime Kummer defined a character  $\psi_j(\mathfrak{p})$  as follows:  $\mathfrak{p} = N_{L/K} \mathfrak{P}$  is an ideal in  $\mathbf{Z}[\zeta]$ ,  $\mathfrak{p}^h = (\pi)$  is principal, and if we insist on taking  $\pi$  primary, then the symbol  $\left(\frac{\pi}{\mathfrak{p}_j}\right)$  only depends on  $\mathfrak{P}$ . We put

$$\psi_j(\mathfrak{P}) = \left(\frac{N_{L/K} \mathfrak{P}}{\mathfrak{p}_j}\right) := \left(\frac{\pi}{\mathfrak{p}_j}\right)^{h^*},$$

where  $h^*$  is an integer such that  $h^*h \equiv 1 \pmod{\ell}$ .

In total there are now  $\rho + t$  characters, and these can be shown<sup>57</sup> to depend only on the ideal class of  $\mathfrak{P}$ . The ideal classes with trivial characters form a subgroup  $C_{\text{gen}}^z$  in  $\text{Cl}^z(L)$ , the class group of the order  $\mathcal{O}_z$ , and  $C_{\text{gen}}^z$  is called the principal genus. The quotient group  $\text{Cl}_{\text{gen}}^z(L/K) = \text{Cl}^z(L)/C_{\text{gen}}^z$  is called the genus class group, and the main problem of determining its order is solved by invoking ambiguous ideal classes:

The number of existing genera is not greater than the number of all essentially different nonequivalent ambiguous classes.<sup>58</sup>

In forty pages,<sup>59</sup> Kummer then showed that there are exactly  $\ell^{\rho+t-1}$  ambiguous ideal classes. This is quite striking, because the usual ambiguous class number formulas all contain a unit index as a factor. It is Kummer's peculiar choice of the order he is working in which eliminates this index; by working in an order with a nontrivial conductor Kummer is actually able to simplify genus theory considerably. But as the number of pages shows, he had to work hard nonetheless.

The upshot is the first inequality of genus theory in Kummer's setting: there are at most  $\ell^{\rho+t-1}$  genera.<sup>60</sup> Kummer noted, however, that this is not good enough to prove the reciprocity law: imitating Gauss's second proof only gives a distinction between  $\ell$ -th power residues and nonresidues, that is, a statement to the effect that  $\left(\frac{\alpha}{\beta}\right)_\ell = 1$  for primary  $\alpha, \beta \in \mathbf{Z}[\zeta_\ell]$  if and only if  $\left(\frac{\beta}{\alpha}\right)_\ell = 1$ . Kummer closed this gap by proving the second inequality in some special cases. To this end, he effectively studied norm residues modulo powers of  $(1 - \zeta)$  in the Kummer extensions  $\mathbf{Q}(\zeta, \sqrt[\ell]{\mu})/\mathbf{Q}(\zeta)$ . His first result ([Kummer 1859], p. 805) was that if  $\alpha \in \mathbf{Z}[\zeta]$  is a norm from  $\mathcal{O}_w$ , then

$$\mathcal{L}^1(\alpha)\mathcal{L}^{\ell-1}(\mu) + \mathcal{L}^2(\alpha)\mathcal{L}^{\ell-2}(\mu) + \mathcal{L}^{\ell-1}(\alpha)\mathcal{L}^1(\mu) \equiv 0 \pmod{\ell}. \quad (*)$$

This means that a certain element of  $\mathbf{F}_\ell$  vanishes if  $\alpha$  is a norm from  $\mathcal{O}_w$ . Hilbert later realized that the left hand side is just the additively written norm residue symbol

57. See [Kummer 1859], p. 748.

58. See [Kummer 1859], p. 751: *Die Anzahl aller wirklich vorhandenen Gattungen ist nicht größer, als die Anzahl aller wesentlich verschiedenen, nicht äquivalenten ambigen Klassen.*

59. See [Kummer 1859], pp. 752–796.

60. See [Kummer 1859], p. 796, statement (V). Kummer writes  $\lambda$  instead of our  $\ell$ .

at the prime  $\mathfrak{p}$  above  $p$ . In [Kummer 1859], p. 808, Kummer showed that condition (\*) is equivalent to

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

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

The first special case was obtained on p. 811 of [Kummer 1859]: if  $t = 1$ , and if the ramified prime ideal has a special property, then there are exactly  $\ell^\rho$  genera. On p. 817, he derived a similar result for certain Kummer extensions with exactly two ramified primes. This turned out to be sufficient for proving the reciprocity laws, but before Kummer did so, he applied these reciprocity laws to derive the general principal genus theorem:

The number of existing genera in the theory of ideal numbers in  $z$  is equal to the  $\ell$ -th part of all total characters.<sup>61</sup>

### 9. Hilbert and the Kummer Field

Hilbert's *Zahlbericht* [Hilbert 1897] consists of five parts: the foundations of ideal theory, Galois theory, quadratic number fields, cyclotomic fields, and Kummer extensions. 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, with finding a good definition of the norm residue symbol, and with incorporating Kummer's special results on genus theory of Kummer extensions into a theory which is on a par with the genus theory of binary quadratic forms in sec. 5 of Gauss's *Disquisitiones Arithmeticae*.

The quadratic norm residue symbol  $\left(\frac{n, m}{p}\right)$  is defined to be +1 if  $m$  is a square or if  $n$  is congruent modulo every power of  $p$  to the norm of a suitable integer from  $\mathbf{Q}(\sqrt{m})$ , and  $\left(\frac{n, m}{p}\right) = -1$  otherwise. This Hilbert symbol can be expressed using generalized Legendre symbols; in [Hilbert 1899], § 9, *Satz 13*, Hilbert derived the formula

$$\left(\frac{v, \mu}{\mathfrak{p}}\right) = \left(\frac{(-1)^{ab} \rho \sigma}{\mathfrak{p}}\right)$$

for primes  $\mathfrak{p}$  not dividing 2 in number fields  $k$ , where  $\mathfrak{p}^a \parallel \mu$ ,  $\mathfrak{p}^b \parallel v$ , and  $v^a \mu^{-b} = \rho \sigma^{-1}$  for integers  $\rho, \sigma \in \mathcal{O}_k$  coprime to  $\mathfrak{p}$ .

To define the  $\ell$ -th power norm residue symbol for odd primes  $\ell$ , Hilbert proceeded the other way around. Let  $v_{\mathfrak{p}}$  be the discrete valuation associated to the prime ideal  $\mathfrak{p}$ . Writing  $v^{v_{\mathfrak{p}}(\mu)} \mu^{-v_{\mathfrak{p}}(v)} = \rho \sigma^{-1}$  with integers  $\rho, \sigma \in \mathcal{O}_k$  such that  $v_{\mathfrak{p}}(\rho) = v_{\mathfrak{p}}(\sigma) = 0$ , he defined for prime ideals  $\mathfrak{p}$  not dividing  $\ell$ :

$$\left(\frac{v, \mu}{\mathfrak{p}}\right)_{\ell} = \left(\frac{\rho}{\mathfrak{p}}\right)_{\ell} \left(\frac{\sigma}{\mathfrak{p}}\right)_{\ell}^{-1}.$$

---

61. See [Kummer 1859], p. 825: *Die Anzahl der wirklich vorhandenen Gattungen der idealen Zahlen in  $z$  ist genau gleich dem  $\ell$ -ten Theile aller Gesamtcharaktere.*

The definition of the norm residue symbol for prime ideals  $\mathfrak{p} \mid \ell$  is much more involved; in his *Zahlbericht*, Hilbert only considered the case  $k = \mathbf{Q}(\zeta_\ell)$  and used Kummer's differential logarithms in the case  $\ell \geq 3$ : for  $\mu \equiv \nu \equiv 1 \pmod{\ell}$ , he put (compare Kummer's result (\*) above)

$$\left(\frac{\nu, \mu}{\mathfrak{l}}\right)_\ell = \zeta^S \text{ with } S = \mathcal{L}^1(\nu)\mathcal{L}^{\ell-1}(\mu) - \mathcal{L}^2(\nu)\mathcal{L}^{\ell-2}(\mu) \pm \dots - \mathcal{L}^{\ell-1}(\nu)\mathcal{L}^1(\mu),$$

and then extended it to  $\mu, \nu$  coprime to  $\ell$  by

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

Hilbert's genus theory then went as follows.<sup>62</sup> Let  $k = \mathbf{Q}(\zeta_\ell)$ , and assume that the class number  $h$  of  $k$  is not divisible by  $\ell$ . Consider the Kummer extension  $K = k(\sqrt[\ell]{\mu})$ . Let  $\mathfrak{p}_1, \dots, \mathfrak{p}_t$  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

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

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

In [Hilbert 1897], *Satz 150*, Hilbert generalized Gauss's work 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  $\ell$  if  $\mathfrak{p} \neq \mathfrak{l}$  is ramified or if  $\mathfrak{p} = \mathfrak{l}$  and  $e > \ell$ . In the following *Satz 151*, Hilbert showed that his symbol defined in terms of power residue symbols actually is a norm residue symbol. Following Gauss, Hilbert first<sup>63</sup> derived the inequality  $g \leq a$  between the number of genera and ambiguous ideal classes, then<sup>64</sup> proved the reciprocity law  $\prod_v \left(\frac{a, b}{v}\right) = 1$  for the  $\ell$ -th power Hilbert symbol and regular primes  $\ell$ , and finally<sup>65</sup> obtained the second inequality  $g \geq a$ . This result is then used for proving the principal genus theorem:

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  $k(\zeta)$ .<sup>66</sup>

62. We rewrite it slightly using the concept of quotient group which Hilbert avoids.

63. See [Hilbert 1897], *Hilfssatz 34*.

64. See [Hilbert 1897], § 160.

65. See [Hilbert 1897], *Satz 164*.

66. See [Hilbert 1897], *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.

This implies the familiar equality  $C_{\text{gen}} = \text{Cl}(K)^{1-\sigma}$  if we work with  $\ell$ -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 concluded this section with the following remark, which blissfully passes over the difference between the Gaussian language of quadratic forms and its translation into algebraic number theory:

Thus we have succeeded in transferring all those properties to the regular Kummer field that have been stated and proved for the quadratic number field already by Gauss.<sup>67</sup>

## 10. Philipp Furtwängler

In Philipp Furtwängler's construction of Hilbert class fields, the following Principal Genus Theorem played a major role:<sup>68</sup>

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

To a cohomologically trained eye, this looks deceptively like the vanishing of  $H^{-1}(G, \text{Cl}(L))$ , but it is not. Indeed, one has  $H^{-1}(G, \text{Cl}(L)) \neq 0$  in general. The point is that there is a difference between the relative norm  $N_{L/K} : \text{Cl}(L) \rightarrow \text{Cl}(K)$  and the algebraic norm

$$\nu_{L/K} = 1 + \sigma + \sigma^2 + \dots + \sigma^{(L:K)-1} : \text{Cl}(L) \rightarrow \text{Cl}(L).$$

The connection between them is  $\nu = j \circ N$ , where  $j : \text{Cl}(K) \rightarrow \text{Cl}(L)$  is the transfer of ideal classes. This means that Furtwängler's principal genus theorem cannot be translated easily into the cohomological language; ideal classes may capitulate. Furtwängler used his principal genus theorem in [Furtwängler 1916] 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  $L/K$ .<sup>69</sup>

67. See [Hilbert 1897], § 165, last sentence: *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.* For connections between genus theory and reciprocity laws see also [Skolem 1928].

68. Hilbert's version of the Principal Genus Theorem discussed above characterizes  $\text{Cl}(L)^{1-\sigma}$  for cyclic extensions  $K/k$  of degree  $\ell$  in cases where the  $\ell$ -class number of the base field  $K$  is trivial. Furtwängler's result, which is *Satz 1* of [Furtwängler 1906], characterizes the group  $\text{Cl}(L)^{1-\sigma}$  for unramified cyclic extensions  $L/K$ , in which the class number of the base field is necessarily divisible by  $\ell$ .

69. We will mention below the cohomological interpretation of this result in terms of the idèle class group. Because of this interpretation, Kubota credited Furtwängler with the "fully idèle-theoretic" result in the case of Kummer extensions of prime degree – see [Kubota 1989]. In the same paper, Kubota showed that the second inequality of class field theory

## 11. Teiji Takagi and Helmut Hasse

In this section, we assume some familiarity with class field theory in its classical formulation. 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  $(\alpha)$  in  $K$  with  $\alpha \equiv 1 \pmod{\mathfrak{m}}$ , let  $D_K\{\mathfrak{m}\}$  denote the group of ideals in  $K$  coprime to  $\mathfrak{m}$ , and let  $D_L\{\mathfrak{m}\}$  denote the corresponding object for  $L$ . 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 Heinrich 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. The *first inequality*  $(D_K\{\mathfrak{m}\} : H_{L/K}\{\mathfrak{m}\}) \leq (L : K)$  holds for any finite extension  $L/K$  and any modulus  $\mathfrak{m}$  and can be proved rather easily using analytic techniques. The *second inequality* says that  $(D_K\{\mathfrak{f}\} : H_{L/K}\{\mathfrak{f}\}) \geq (L : K)$  for any cyclic extension  $L/K$  of prime degree  $\ell$ , and where  $\mathfrak{f}$  is the conductor of  $L/K$ , that is, the ideal such that the relative discriminant of  $L/K$  is  $\mathfrak{f}^{\ell-1}$ .

In his 1932–1933 Marburg lectures on class field theory, Helmut Hasse put the proof of the second inequality into historical perspective by mentioning the role of Gauss's work:

We now are aiming at 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 the D.A.<sup>70</sup>

The relative discriminant of a cyclic extension  $L/K$  of prime degree  $\ell$  equals  $\mathfrak{f}^{\ell-1}$ , 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 a connection between the class group  $\text{Cl}(L)$  and some ray class group  $\text{Cl}_K^v$  defined modulo  $\mathfrak{f}$ : given a class  $c = [\mathfrak{A}] \in \text{Cl}(L)$ , we can form the ray class  $[N_{L/K}\mathfrak{A}]$  in the group  $\text{Cl}_K^v$  of ideals modulo norm residues, that is, in the group  $D_K\{\mathfrak{f}\}$  of ideals coprime to  $\mathfrak{f}$  modulo the group  $P_K^v\{\mathfrak{f}\}$  of principal ideals generated by norm residues modulo the conductor  $\mathfrak{f}$ ; 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  $N_{L/K}\lambda \in P_K^v\{\mathfrak{f}\}$ .

The image of the norm map  $N_{L/K} : \text{Cl}(L) \rightarrow \text{Cl}_K^v$  is  $H_{L/K}\{\mathfrak{f}\}/P_K^v\{\mathfrak{f}\}$ , and thus involves the ideal group associated with  $L/K$ . The kernel of the norm map is called the principal genus  $C_{\text{gen}}$ ; it is the group of all ideal classes  $c = [\mathfrak{A}] \in \text{Cl}(L)$

---

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.

70. See [Hasse 1967], p. 151: *Wir gehen jetzt auf den Beweis des Umkehrsatzes aus. Die dazu erforderlichen Überlegungen des laufenden Paragraphen bilden die Verallgemeinerung der berühmten Gauss'schen Untersuchungen über die Theorie der Geschlechter quadratischer Formen aus seinen Disquisitiones Arithmeticae.*

such that  $N_{L/K}\mathfrak{A} = (\alpha)$  for norm residues  $\alpha \in K^\times$  (i.e.,  $\alpha$  is coprime to  $\mathfrak{f}$  and a norm residue at every prime ideal). This gives the exact sequence

$$1 \longrightarrow C_{\text{gen}} \longrightarrow \text{Cl}(L) \xrightarrow{N} H_{L/K}\{\mathfrak{f}\}/P_K^\nu\{\mathfrak{f}\} \longrightarrow 1. \quad (**)$$

Thus computing the number of genera  $g = (\text{Cl}(L) : C_{\text{gen}})$  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,  $C_{\text{gen}}$  clearly contains the group  $\text{Cl}(L)^{1-\sigma}$ , where  $\sigma$  is a generator of  $\text{Gal}(L/K)$ . This shows that

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

that is, the first inequality of genus theory. Its 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  $h_K = \#\text{Cl}(K)$  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  $E_\nu$  its subgroup of units that are norm residues modulo  $\mathfrak{f}$ .

To prove the second inequality of genus theory:  $g \geq a$ , we use the exact sequence (\*\*) and get

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

The index in the denominator satisfies  $(D_K\{\mathfrak{f}\} : H_{L/K}\{\mathfrak{f}\}) \leq \ell$  by the first inequality. The index in the numerator is the product of  $h_K = (D_K\{\mathfrak{f}\} : P_K\{\mathfrak{f}\})$ , the class number of  $K$ , by the index  $(P_K\{\mathfrak{f}\} : P_K^\nu\{\mathfrak{f}\})$ . This index can be computed explicitly:

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

Therefore  $(D_K\{\mathfrak{f}\} : P_K^\nu\{\mathfrak{f}\}) = (E_\nu : E \cap NL^\times) \cdot a\ell \geq a\ell$ , and we have equalities throughout in the sequence of inequalities

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

Thus  $(D_K\{\mathfrak{f}\} : H_{L/K}\{\mathfrak{f}\}) = \ell$ , and *cyclic extensions are class fields*. Next we get the

**Principal Genus Theorem.**<sup>71</sup>  $C_{\text{gen}} = \text{Cl}(L)^{1-\sigma}$ .

71. If  $L/K$  is unramified, then  $C_{\text{gen}} = \text{Cl}(L)[N]$  coincides with the kernel of the norm map  $\text{Cl}(L) \longrightarrow \text{Cl}(K)$ , and the principal genus theorem becomes the Theorem of § 10 above.

Finally, we also obtain the *norm theorem for units*:  $(E_v : E \cap NL^\times) = 1$ , i.e., each unit that is a norm residue modulo the conductor is the norm of some element of  $L^\times$ .

Takagi derived the norm theorem – to the effect that in cyclic extensions norm residues modulo the conductor are actual norms – from the principal genus theorem. In his *Klassenkörperbericht* [Hasse 1927], Hasse reproduced Takagi's proof of the second inequality with only minor modifications. But in his 1932 Marburg lectures [Hasse 1967], he established the second inequality

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

directly by a different route. The main advantage of this arrangement of proof is that it is valid for finite cyclic extensions of arbitrary degree. Furthermore, the full norm theorem is a consequence of equality in  $(***)$ , and the new proof does not use the first inequality. This last fact would later allow Claude 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  $(***)$ , 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). In this way, Hasse's norm theorem – which follows by comparing  $(***)$  with the first inequality – contains the principal genus theorem.

Recall that ideal classes in  $L$  are mapped by the norm to ray classes modulo  $\mathfrak{f}$  in  $K$ . The question arises whether more generally ray classes in  $L$  can be linked to ray classes in  $K$ . This was established by Hasse's General principal genus theorem.<sup>72</sup> In order to state it for a cyclic extension of prime degree  $L/K$  with Galois group generated by  $\sigma$ , one needs, for a given modulus  $\mathfrak{m}$  in  $K$ , a  $\sigma$ -invariant modulus  $\mathfrak{M}$  in  $L$  dividing  $\mathfrak{m}$  such that for  $\beta \in L^\times$  coprime to  $\mathfrak{M}$  we have  $N_{L/K}(\beta) \equiv 1 \pmod{\mathfrak{m}}$  if and only if  $\beta \equiv \alpha^{1-\sigma} \pmod{\mathfrak{M}}$ . Using this, Hasse defined the principal genus  $\overline{H}_1 \pmod{\mathfrak{M}}$  in  $L$  to be the group of ray classes modulo  $\mathfrak{M}$  whose relative norms land in the ray modulo  $\mathfrak{m}$  in  $K$ . With this notation the General Principal Genus Theorem states that *the principal genus  $\overline{H}_1$  coincides with the group of  $(1 - \sigma)$ -th powers of ray classes mod  $\mathfrak{M}$  in  $L$ .*<sup>73</sup>

## 12. Nikolai Grigorievich Čebotarev and Arnold Scholz

The generalization of genus theory from cyclic to arbitrary normal extensions was mainly the work of Nikolai Grigorievich Čebotarev and Arnold Scholz.<sup>74</sup>

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  $L_{\text{gen}}$  of  $L$  with respect to  $K$ ; the maximal unramified extension which is central over  $K$  is called the central class field and is denoted by  $L_{\text{cen}}$ .

According to Scholz, these definitions are contained in [Čebotarev 1929]; the characterization of the genus and central class fields in terms of class groups is due

72. See [Hasse 1927], pp. 304–310.

73. This was further generalized by Herbrand – see [Herbrand 1932].

74. See [Čebotarev 1929] and [Scholz 1940].

to Scholz, who used the following theorem to generalize Hasse's norm theorem – everywhere local norms are global norms – to all extensions whose Galois groups have trivial Schur multiplier:<sup>75</sup>

**Theorem.** 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.<sup>76</sup> Then the class field associated to the ideal group  $H$  is the genus class field  $L_{\text{gen}}$ , and the class field associated to  $N$  is the central class field  $L_{\text{cen}}$ . In particular, Scholz's number knot  $H_0/N_0$  is isomorphic to the Galois group of  $L_{\text{cen}}/L_{\text{gen}}$ .

Being an unramified abelian extension of  $L$ ,  $L_{\text{gen}}$  corresponds to some quotient  $\text{Cl}(K)/C_{\text{gen}}$  of the class group of  $K$ . This group  $C_{\text{gen}}$  is called the *principal genus*. For cyclic extensions  $L/K$ , it satisfies  $C_{\text{gen}} = \text{Cl}(L)^{1-\sigma}$ , for  $\sigma$  a generator of  $\text{Gal}(L/K)$ .

The following theorem – called the *classical principal genus theorem* in [Fröhlich 1983], pp. 18–19 – connects the modern definition of the principal genus with the classical one by Takagi:

**Theorem.** Let  $L/K$  be a cyclic extension, and  $\sigma$  a generator of  $\text{Gal}(L/K)$ . 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 refer to [Hasse 1951], [Leopoldt 1953], [Gold 1975], [Stark 1976] (this generalization of genus theory lacks an analogue of Gauss's principal genus theorem), [Gurak 1977], and [Razar 1977].

### 13. Emmy Noether

In 1932, Emmy Noether was invited to deliver a lecture at the International Congress of Mathematicians in Zürich. She devoted this lecture to two new illustrations of the usefulness of the then flourishing theory of algebras:<sup>77</sup>

I would like to report today on this relevance of the noncommutative for the commutative; more precisely, I would like to trace this phenomenon in detail for two classical questions which go back to Gauss: the Principal Genus Theorem and the closely related Norm Theorem. These questions have changed again and again in the course of time: with Gauss they appear as the conclusion of his theory of quadratic forms; then they play an essential part in characterizing relatively cyclic and abelian number fields, and they can finally be stated as theorems on automorphisms and on

75. Cf. Jehne's more modern presentation and generalization in [Jehne 1979].

76. Observe that  $H$  is the principal genus in the sense of Takagi.

77. The footnotes in [Noether 1932] give a vivid impression of the activity of the theory of algebras at the time. In [Noether 1932], § 4, the Norm Theorem is related to the Brauer-Hasse-Noether Theorem. Cf. [Fenster, Schwermer 2005], and [Hasse & Noether 2006].

the splitting of algebras. It is this latter formulation which yields a transfer of these theorems to arbitrary relatively abelian number fields.<sup>78</sup>

The noncommutative algebras are thus presented by Emmy Noether as the stepping stone to generalize arithmetic theorems from cyclic to abelian extensions. To generalize the Principal Genus Theorem, she therefore starts with crossed products.<sup>79</sup>

Let  $K$  be a field and  $L/K$  a separable extension of degree  $n$  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  $A$ . As an  $L$ -vector space,  $A$  is generated by basis elements  $u_{\sigma_1}, \dots, u_{\sigma_n}$  corresponding to the group elements  $\sigma_i : A = u_{\sigma_1}L \oplus \dots \oplus u_{\sigma_n}L$ . It is required that  $z^\sigma = u_{\sigma}^{-1}zu_{\sigma}$  hold for every  $z \in L$ . This defines a *factor system*  $(a_{\sigma,\tau})$  in  $L^\times$  by the formulae  $u_{\sigma}u_{\tau} = u_{\sigma\tau}a_{\sigma,\tau}$ , and associativity of multiplication gives the cocycle relation  $a_{\sigma\tau,\rho}a_{\sigma,\tau}^\rho = a_{\sigma,\tau\rho}a_{\tau,\rho}$ . The product

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

makes  $A$  into a simple normal algebra over  $K$  which is denoted by  $A = (a_{\sigma,\tau}, L, G)$ . Different factor systems  $a_{\sigma,\tau}$  and  $\bar{a}_{\sigma,\tau}$  generate isomorphic algebras if there are  $c_{\sigma} \in L^\times$  such that  $\bar{a}_{\sigma,\tau} = a_{\sigma,\tau}c_{\sigma}^{\tau}c_{\tau}/c_{\sigma\tau}$ . The cosets  $u_{\sigma}L^\times$  define a group extension  $G^\times$  of  $G$  by  $L^\times$ .

Emmy Noether published a detailed account of her Principal Genus Theorem in [Noether 1933]. The first result there, which she called the *Hauptgeschlechtssatz im Minimalen*, i.e., Minimal Principal Genus Theorem, was formulated, for a finite Galois extension  $L/K$  with Galois group  $G$ , in three equivalent variants:<sup>80</sup>

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  $b \in L^\times$  such that  $c_{\sigma} = b^{1-\sigma}$  for all  $\sigma \in G$ .

78. See [Noether 1932], § 1: *Über diese Bedeutung des Nichtkommutativen für das Kommutative möchte ich heute berichten: und zwar will ich das im einzelnen verfolgen an zwei klassischen, auf Gauss zurückgehenden Fragestellungen, dem Hauptgeschlechtssatz und dem eng damit verbundenen Normensatz. Diese Fragestellungen haben sich im Laufe der Zeit immer wieder gewandelt: bei Gauss treten sie auf als Abschluss seiner Theorie der quadratischen Formen; dann spielen sie eine wesentliche Rolle bei der Charakterisierung der relativ zyklischen und abelschen Zahlkörper durch die Klassenkörpertheorie, und schliesslich lassen sie sich aussprechen als Sätze über Automorphismen und über das Zerfallen von Algebren, und diese letztere Formulierung gibt dann zugleich eine Übertragung der Sätze auf beliebige relativ galoissche Zahlkörper.*

79. Cf. [Noether 1932], § 3; except for the letters used to denote Galois automorphisms, our notations are the same as Noether's. More technical details are given in the preprint version <http://www.math.uiuc.edu/Algebraic-Number-Theory/0354/> of this chapter, and will be published elsewhere.

80. See [Noether 1933], p. 414-415. This article was already announced in her Zürich talk, and was submitted on October 27, 1932.

Diese Hauptideale  $(a_S, \tau)$  bilden im Sinne der Verknüpfung der Faktorensysteme eine Gruppe; diese Gruppe umfaßt die Transformationsgrößen  $(c_S^T)(c_T)/(c_{ST})$ ; denn die Faktorensysteme  $c_S^T c_T / c_{ST}$  erzeugen überall zerfallende Algebren.

2. *Formulierung des Hauptgeschlechtssatzes.* Ich spreche den Satz entsprechend dem Satz im Minimalen in drei gleichbedeutenden Fassungen aus.

Erste Fassung: *Entsteht, bei Zugrundelegung der induzierten Idealklasseneinteilung der Faktorensysteme, durch die Substitutinn  $v_S = u_S \bar{c}_S$ <sup>12)</sup> ein Automorphismus der  $n$  Komplexe  $\{\dots u_S \bar{\mathfrak{S}} \dots\}$  — d. h. bestehen für  $v_S$  im Sinne dieser Klasseneinteilung dieselben Relationen (3) — so ist dieser Automorphismus ein innerer und wird durch eine Idealklasse  $\bar{b}$  erzeugt.*

Zweite Fassung: *Gehören die aus den Idealklassen  $\bar{c}_S$  gebildeten Transformationsgrößen  $\bar{c}_S^T \bar{c}_T / \bar{c}_{ST}$  sämtlich der Hauptklasse der induzierten Klasseneinteilung der Faktorensysteme an — die Gesamtheit dieser „Vektoren“  $\{\dots \bar{c}_S \dots\}$  aus Idealklassen bildet das Hauptgeschlecht —, so sind die Klassen  $\bar{c}_S$  symbolische  $(1-S)$ -te Potenzen; d. h. es gibt eine Idealklasse  $\bar{b}$  derart, daß  $\bar{c}_S = \bar{b}^{1-S} = \bar{b} / \bar{b}^S$  für alle  $S$  aus  $\mathfrak{G}$ .*

Dritte Fassung: *Bei Zugrundelegung der induzierten Idealklasseneinteilung für die Faktorensysteme besitzt die Gruppe  $\mathfrak{G}$  nur eine einzige, zur Einsklasse der Faktorensysteme gehörige verschränkte Darstellungsclassen ersten Grades in  $\bar{\mathfrak{S}}$ .*

Daß die verschiedenen Fassungen gleichbedeutend sind, folgt wie in §1; der Übergang von der ersten zur zweiten Fassung wird noch einfacher, da der Automorphismus schon durch  $v_S = u_S \bar{c}_S$  erzeugt vorausgesetzt ist. Diese Voraussetzung ist notwendig, da jetzt  $\bar{\mathfrak{S}}$  nicht mehr größte kommutative Untergruppe zu sein braucht (es können alle Klassen von  $\bar{\mathfrak{S}}$  ambig sein). Zu der dritten Fassung ist zu bemerken, daß als Darstellungsmatrizen, da in  $\bar{\mathfrak{S}}$  nur multiplikative Verknüpfung definiert ist, jetzt nur solche auftreten, die in jeder Zeile und Spalte nur ein von Null verschiedenes Element enthalten; für Darstellungen ersten Grades ist das keine Einschränkung.

3. *Beweis des Hauptgeschlechtssatzes.* Ich gebe den Beweis der zweiten Fassung. Der Beweis beruht auf zwei Hilfssätzen.

Hilfssatz 1. (Hauptgeschlechtssatz der Ideale): *Ergeben die aus den Idealen  $c_S$  gebildeten Transformationsgrößen  $c_S^T c_T / c_{ST}$  das Einheitsideal, so sind die  $c_S$  symbolische  $(1-S)$ -te Potenzen;  $c_S = \bar{b}^{1-S}$  für alle  $S$  aus  $\mathfrak{G}$ . Gleichbedeutend damit ist wieder die erste und dritte Fassung, wobei in der ersten Fassung, wie bei den Idealklassen, der Automorphismus als durch  $v_S = u_S c_S$  erzeugt vorausgesetzt werden muß.*

<sup>12)</sup>  $\bar{c}_S$  bedeutet die Idealklasse von  $c_S$ .

3. The group  $G$  has a unique crossed representation class of the first degree associated to the trivial factor system.

Here (in 3.) a representation  $u_\sigma \mapsto C_\sigma$  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  $u_\sigma \mapsto C_\sigma$  and  $u_\sigma \mapsto D_\sigma$  for  $a_{\sigma,\tau}$  belong to the same class if  $C_\sigma = B^{-\sigma} D_\sigma B$ .

In the slightly more modern language of Galois cohomology groups, version 2. of the minimal principal genus theorem claims that  $H^1(G, L^\times) = 0$ . This is Speiser's generalization of Hilbert's *Satz 90* of [Hilbert 1897], from cyclic to arbitrary finite Galois extensions.

In § 2 of [Noether 1933], Noether considered what we may call an *ideal factor system* of a Galois extension  $L/K$  with Galois group  $\text{Gal}(L/K) = \{\sigma, \tau, \dots\}$ , i.e., a system of  $n^2$  ideals  $\mathfrak{a}_{\sigma,\tau}$  of  $L$  satisfying the cocycle relations

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

Given  $n$  ideals  $\mathfrak{c}_\sigma$ , one obtains the so-called *transformation system*  $\mathfrak{a}_{\sigma,\tau} = \frac{\mathfrak{c}_\sigma^\tau \mathfrak{c}_\tau}{\mathfrak{c}_{\sigma\tau}}$ .

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)  $\mathfrak{a}_{\sigma,\tau} = (a_{\sigma,\tau})$ , and (2)  $a_{\sigma,\tau}$  determines an algebra  $\mathfrak{A} = (L, a)$  which splits at every ramified place  $\mathfrak{p}$  of  $L/K$ . With this notation, we have version 2. of

**Emmy Noether's Principal Genus Theorem.**<sup>81</sup> 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  $\sigma \in \text{Gal}(L/K)$ .

Noether's proof of this result follows easily from two lemmas, of which the second<sup>82</sup> is a variant of the Brauer-Hasse-Noether theorem on the local characterization of the splitting of semi-simple algebras, whereas the first one is Noether's Principal Genus Theorem for Ideals.<sup>83</sup> In terms of Galois cohomology of the normal extension of number fields  $L/K$  with Galois group  $G$ , writing  $D_L$  for the group of fractional ideals in  $L$ , the latter theorem amounts to the statement that  $H^1(G, D_L) = 0$ .

Noether's formulation of the principal genus theorem was apparently not very influential, but there have been a few articles picking up her ideas; we mention [Terada 1952], [Terada 1953], [Kunihishi, Takahashi 1953], as well as [Tannaka 1958]. Let us briefly sketch here two modern reformulations of Noether's Theorems. Peter Roquette has proposed<sup>84</sup> the following translation of Noether's results into the language of Galois cohomology of idèles.

81. For all three versions 1.–3. and their equivalence, see [Noether 1933], p. 417.

82. See [Noether 1933], *Hilfssatz 2*, p. 418.

83. See [Noether 1933], *Hilfssatz 1*, p. 417, for the statement in terms of transformation systems. Noether gives a direct four line proof of this *Hilfssatz 1* due to Emil Artin.

84. In an email to the author dated June 14, 2001.

We fix a normal extension  $L/K$  of number fields with Galois group  $G = \text{Gal}(L/K)$ . All our cohomology groups will be formed with  $G$ , so we write simply  $H^q(M)$  for  $H^q(G, M)$ . Let  $S$  be the set of primes of  $L$  ramified in  $L/K$ . Let  $H_S^2(L^\times)$  denote the subgroup of  $H^2(L^\times)$  whose elements split at all primes in  $S$ ; in other words,  $H_S^2(L^\times)$  is the kernel of the natural map  $H^2(L^\times) \rightarrow H^2(\prod_{w \in S} L_w^\times)$  induced by  $L^\times \rightarrow \prod_{w \in S} L_w^\times$ .

The exact sequence  $1 \rightarrow E_L \rightarrow L^\times \rightarrow P_L \rightarrow 1$ , where  $P_L$  denotes the group of principal ideals and  $E_L$  the units in  $L$ , yields a map  $H_S^2(L^\times) \rightarrow H^2(P_L)$  whose image we denote simply by  $H_S$ .

The sequence  $1 \rightarrow P_L \rightarrow D_L \rightarrow \text{Cl}_L \rightarrow 1$  defining the ideal class group of  $L$  gives us the following exact sequence whose first term is 0 in view of Noether's Principal Genus Theorem for Ideals:

$$0 = H^1(D_L) \rightarrow H^1(\text{Cl}_L) \rightarrow H^2(P_L) \rightarrow H^2(D_L).$$

This identifies  $H^1(\text{Cl}_L)$  with a subgroup of  $H^2(P_L)$ , and we can formulate:

**Noether's Principal Genus Theorem.**  $H_S \cap H^1(\text{Cl}) = 0$ .

To see the connection with Noether's original formulation, observe that a transformation system  $c_\sigma$  of ideals is a cocycle of the ideal class group and therefore defines an element  $c_\sigma \in H^1(\text{Cl}_L)$  if  $[c_\sigma]^\tau [c_\tau] = [c_{\sigma\tau}]$  (this is the first condition of the system  $c_\sigma$  being in the principal class). The requirement that  $c_\sigma = [c_\sigma] = [b]^{1-\sigma}$  says that the cocycle is a coboundary. Thus  $H^1(\text{Cl}_L) = 1$ . However, this is only true if the second condition is also satisfied; this condition requires that  $c_\sigma^\tau c_\tau c_{\sigma\tau}^{-1} = (a_{\sigma,\tau})$  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  $c_\sigma \in H^1(\text{Cl}_L)$  defines a factor set of principal ideals in  $H^2(P_L)$  under the connecting homomorphism; if this factor system actually comes from an element  $a_{\sigma,\tau} \in H^2(L^\times)$  whose associated algebra splits at the ramified primes – i.e., if  $a_{\sigma,\tau} \in H_S^2(L^\times)$  – then Noether's principal genus theorem claims that the element  $c_\sigma$  is trivial.

Albrecht Fröhlich's article [Fröhlich 1983] contains a cohomological interpretation of Noether's principal genus theorem that differs slightly from Roquette's. Let  $J'_L \simeq \prod_{w \in S} L_w^\times$  denote idèles having entries 1 outside of  $S$ . The projection from all idèles  $J_L \rightarrow J'_L$  and the inclusion  $L^\times \rightarrow J_L$  give rise to maps  $\pi_1 : H^2(J_L) \rightarrow H^2(J'_L)$  and  $\iota : H^2(L^\times) \rightarrow H^2(J_L)$  such that  $\ker \pi_1 \circ \iota = H_S^2(L^\times)$ . Fröhlich defines maps  $\psi : H^2(L^\times) \rightarrow H^2(P_L)$  and  $\phi : H^2(P_L) \rightarrow H^2(D_L)$  such that  $\psi(\ker \pi_1 \circ \iota) = H_S$ . The injectivity of  $H_S^2(L^\times) \rightarrow H^2(D_L)$  then amounts to  $\ker \pi_1 \circ \iota \cap \ker \phi \circ \psi = 0$ , and Fröhlich's version of Noether's theorem reads:

**Theorem.** The following composition of maps is injective:

$$H^1(\text{Cl}_L) \rightarrow H^2(P_L) \rightarrow H^2(P_L)/\psi(\ker \pi_1 \circ \iota).$$

In other words, the induced map  $H^1(\text{Cl}_L) \rightarrow H^2(P_L)/H_S$  is injective. This is, of course, equivalent to the statement that  $H_S \cap H^1(\text{Cl}_L) = 0$  in  $H^2(P_L)$ .

We conclude our survey of the development of the principal genus theorem with Emmy Noether's peculiar acknowledgement of Gauss's *Disquisitiones Arithmeticae*:

Incidentally, in preparation for my Zürich lecture I have read Gauss, for once. It has been said that a halfway educated mathematician knows Gauss's principal genus theorem, but only exceptional people know the principal genus theorem of class field theory. I don't know if that's true – my knowledge went the other way around – but in any case I learned a lot from Gauss about how to view things; above all, that it is good to place the verification of the fact that the classes determined by factor systems are ray classes, at the end; for the transition from my version to Gauss's can be done independently of this, and directly, and it is not before the specialization to class field theory that the conductor is needed. What I am doing is the generalization of the definition of genera via characters.<sup>85</sup>

## Acknowledgements

I would like to thank Peter Roquette for explaining the content of Noether's paper to me.

## References

- ANTROPOV, Alexander A. 1989. On the history of the concept of genus of binary quadratic form (in Russian). *Istoriya i Metodologiya Estestvennykh Nauk* 36, 17–27.
- . 1989. Partitioning of forms by genus and the reciprocity law in L. Euler's work (in Russian). *Voprosy Istorii Estestvoznaniya i Tekhniki* 1, 56–57.
- . 1995. On Euler's partition of forms into genera. *Historia Mathematica* 22, 188–193.
- ARNDT, Friedrich. 1859. Ueber die Anzahl der Genera der quadratischen Formen. *Journal für die reine und angewandte Mathematik* 56, 72–78.
- BELABAS, Karim. 2005. Paramétrisation de structures algébriques et densité de discriminants (d'après Bhargava). In *Séminaire Bourbaki. Vol. 2003–2004*, exposé 935, pp. 267–299. Astérisque 299. Paris: Société mathématique de France.
- BHARGAVA, Manjul. 2004. Higher Composition Laws I, II. *Annals of Mathematics* 159, 217–250, 865–886.
- BUELL, Duncan A. 1989. *Binary Quadratic Forms*. Berlin, Heidelberg, New York: Springer.

85. See [Hasse & Noether 2006]: *Im übrigen habe ich anlässlich der Ausarbeitung meines Züricher Vortrags einmal Gauss gelesen. Es wurde behauptet, daß ein halbwegs gebildeter Mathematiker den Gausssschen Hauptgeschlechtssatz kennt, aber nur Ausnahmefällen 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 Gausssschen 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.* Noether's letter to Hasse of November 25, 1932 (see [Hasse & Noether 2006]) shows that she had plans to further work out her theory. She died, however, in 1935 without ever returning to the topic.

- ČEBOTAREV, Nikolai Grigorievich. 1929. Zur Gruppentheorie des Klassenkörpers. *Journal für die reine und angewandte Mathematik* 161, 179–193.
- DEURING, Max. 1935. *Algebren*. Ergebnisse der Mathematik und ihrer Grenzgebiete 41. Berlin, Heidelberg : Springer.
- DIRICHLET, Johann Peter Gustav LEJEUNE-. 1863. *Vorlesungen über Zahlentheorie*, ed. R. Dedekind. 1<sup>st</sup> ed. 2<sup>nd</sup> ed., 1871. 3<sup>rd</sup> ed., 1879. 4<sup>th</sup> ed., 1894. Braunschweig: Vieweg.
- . 1839. Recherches sur diverses applications de l'analyse infinitésimale à la théorie des nombres. *Journal für die reine und angewandte Mathematik* 19, 324–369. Repr. in *Werke*, ed. L. Kronecker, vol. 1, pp. 411–496. Berlin: G. Reimer, 1889.
- EDWARDS, Harold M. 1977. *Fermat's Last Theorem*. Berlin, Heidelberg, New York: Springer.
- EISENSTEIN, Gotthold. 1844. Théorèmes sur les formes cubiques et solution d'une équation du quatrième degré indéterminée. *Journal für die reine und angewandte Mathematik* 27, 75–79. Repr. in *Mathematische Werke* vol. 1, pp. 1–5. New York: Chelsea, 1975.
- EULER, Leonhard. 1764. De resolutione formularum quadraticarum indeterminatarum per numeros integros. *Novi Commentarii academiae scientiarum imperialis Petropolitanae* 9 (1762–1763), 3–33. Repr. in [Euler 1915], pp. 576–602.
- . 1783. Novae demonstrationes circa divisores numerorum formae  $xx+nyy$ , (E 610), Nov. 20, 1775. *Nova Acta Academiae Scientiarum Imperialis Petropolitanae* 1, 47–74. Repr. in [Euler 1941], pp. 197–220.
- . 1785. De insigni promotione scientiae numerorum, (E 598), Oct. 26, 1775. In *Opuscula analytica* 2, pp. 275–314. St. Petersburg: Typis Academiae Imperialis Scientiarum. Repr. in [Euler 1941], pp. 163–196.
- . 1915. *Opera Omnia*, ed. R. Fueter, vol. I<sub>2</sub>. Leipzig, Berlin: Teubner.
- . 1941. *Opera Omnia*, ed. R. Fueter, vol. I<sub>4</sub>. Leipzig, Berlin: Teubner.
- EULER & GOLDBACH. 1965. *Briefwechsel 1729–1764, von Leonhard Euler und Christian Goldbach*, ed. A.P. Yuškevič, E. Winter. Berlin: Akademie-Verlag.
- FENSTER, Della D., SCHWERMER, Joachim. 2005. A Delicate Collaboration: Adrian Albert and Helmut Hasse and the Principal Theorem in Division Algebras in the early 1930's. *Archive for History of Exact Sciences* 59, 349–379.
- FREI, Günter. 1979. On the development of the genus of quadratic forms. *Annales des Sciences Mathématiques du Québec* 3, 5–62.
- FRÖHLICH, Albrecht. 1981. Algebraic Number Theory. In *Emmy Noether. A Tribute to her Life and Work*, ed. J.W. Brewer, M.K. Smith, pp. 157–163. New York, Basel: Marcel Dekker.
- FUETER, Rudolf. 1941. Vorwort des Herausgebers. In [Euler 1941], pp. vii–xxx.
- FURTWÄNGLER, Philipp. 1906. Eine charakteristische Eigenschaft des Klassenkörpers, Erste Mitteilung. *Göttinger Nachrichten*, 417–434.
- . 1916. Über das Verhalten der Ideale des Grundkörpers im Klassenkörper, *Monatshefte für Mathematik* 27, 1–15.
- GOLD, Robert. 1975. Genera in Abelian extensions. *Proceedings of the American Mathematical Society* 47, 25–28.
- GURAK, Stanley J. 1977. Ideal-theoretic characterization of the relative genus field, *Journal für die reine und angewandte Mathematik* 296, 119–124.

- HASSE, Helmut. 1927. Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper. Teil Ia, Beweise zu I. *Jahresbericht der Deutschen Mathematiker-Vereinigung* 36, 233–311. Repr. (as book) Würzburg, Wien: Physica-Verlag, 3<sup>rd</sup> ed., 1970.
- . 1951. Zur Geschlechtertheorie in quadratischen Zahlkörpern. *Journal of the Mathematical Society of Japan* 3, 45–51.
- . 1967. *Vorlesungen über Klassenkörpertheorie*. Würzburg, Wien: Physica-Verlag.
- HASSE & NOETHER. 2006. *Helmut Hasse – Emmy Noether. Die Korrespondenz 1925 – 1935*, ed. F. Lemmermeyer, P. Roquette. Göttingen: Universitätsverlag.
- HECKE, Erich. 1923. *Vorlesungen über die Theorie der algebraischen Zahlen*. Leipzig: Teubner. Repr. New York: Chelsea, 1948, 1970. Engl. tr. G.U. Brauer, J.R. Goldman, R. Kotzen. Heidelberg, New York: Springer-Verlag, 1981.
- HERBRAND, Jacques. 1932. Sur les théorèmes du genre principal et des idéaux principaux. *Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg* 3, 84–92.
- HILBERT, David. 1894. Über den Dirichletschen biquadratischen Zahlkörper. *Mathematische Annalen* 45, 309–340. Repr. in [Hilbert 1932], pp. 24–52.
- . 1897. Die Theorie der algebraischen Zahlkörper. *Jahresbericht der Deutschen Mathematiker-Vereinigung* 4 (“1894–1895”), 177–546 + Vorwort 1–xviii. Repr. in [Hilbert 1932], pp. 63–363. Eng. tr. by I. Adamson, *The Theory of Algebraic Number Fields*, introd. F. Lemmermeyer, N. Schappacher. New York: Springer, 1998.
- . 1889. Über die Theorie der relativ-Abelschen Zahlkörper. *Nachrichten der Königlichen Gesellschaft der Wissenschaften zu Göttingen*, 370–399. Repr. modified *Acta Mathematica* 26 (1902), 99–132. Repr. in [Hilbert 1932], pp. 483–509.
- . 1899. Über die Theorie des relativquadratischen Zahlkörpers. *Mathematische Annalen* 51, 1–127. Repr. in [Hilbert 1932], pp. 370–482.
- . 1932. *Gesammelte Abhandlungen*, vol. 1. Berlin: Springer. 2<sup>nd</sup> ed., 1970.
- HOFFMAN, J. William, MORALES, Jorge. 2000. Arithmetic of binary cubic forms. *Enseignement Mathématique* 2<sup>nd</sup> ser. 46, 61–94.
- JEHNE, Wolfram. 1979. On knots in algebraic number theory. *Journal für die reine und angewandte Mathematik* 311–312, 215–254.
- JONES, Burton W. 1950. *The Arithmetic Theory of Quadratic Forms*. New York : John Wiley & Sons.
- KRONECKER, Leopold. 1864. Über den Gebrauch der Dirichletschen Methoden in der Theorie der quadratischen Formen. *Monatsberichte der Königlich Preussischen Akademie der Wissenschaften zu Berlin*, 285–303. Repr. in *Werke*, vol. IV, ed. K. Hensel, pp. 227–244. Leipzig: Teubner, 1929.
- KUBOTA, Tomio. 1989. Remarks on the theorems of Takagi and Furtwängler. In *Algebraic Number Theory, in honor of K. Iwasawa. Proceedings of the Workshop “Iwasawa Theory and Special Values of L-Functions,” Berkeley, CA, 1987*, ed. J. Coates, R. Greenberg, B. Mazur, I. Satake, pp. 267–270. *Advanced Studies in Pure Mathematics* 17. Boston, etc.: Academic Press and Tokyo : Kinokuniya.
- KUMMER, Ernst Eduard. 1850. Allgemeine Reziprozitätsgesetze für beliebig hohe Potenzreste. *Monatsberichte der Königlich Preussischen Akademie der Wissenschaften zu Berlin*, 154–165. Repr. in [Kummer 1975], pp. 345–357.

- . 1859. Über die allgemeinen Reziprozitätsgesetze unter den Resten und Nichtresten der Potenzen, deren Grad eine Primzahl ist. *Mathematische Abhandlungen der Königlich-Preussischen Akademie der Wissenschaften zu Berlin*, 19–159. Repr. in [Kummer 1975], pp. 699–839.
- . 1861. Zwei neue Beweise der allgemeinen Reziprozitätsgesetze unter den Resten und Nichtresten der Potenzen, deren Grad eine Primzahl ist. *Mathematische Abhandlungen der Königlich-Preussischen Akademie der Wissenschaften zu Berlin*, 81–122. Repr. *Journal für die reine und angewandte Mathematik* 100 (1887), 10–50. Repr. in [Kummer 1975], pp. 842–882.
- . 1975. *Collected Papers*, ed. A. Weil. vol. 1, *Contributions to Number Theory*. Berlin, Heidelberg etc.: Springer.
- KUNIYOSHI, Hideo, TAKAHASHI, Shuichi. 1953. On the principal genus theorem. *Tohoku Mathematical Journal* 5, 128–131.
- LAGRANGE, Joseph-Louis. 1773. Recherches d'arithmétique. *Nouveaux Mémoires de l'Académie royale des Sciences et Belles-lettres de Berlin, année 1773* (1775), 265–312. Repr. in *Œuvres*, ed. J.-A Serret, vol. III, pp. 695–758. Paris: Gauthier-Villars, 1869; repr. Hildesheim, New York: Georg Olms, 1973.
- . 1774. *Additions aux Eléments d'Algèbre d'Euler*. Lyon: Bruyset, Paris: Desaint. Repr. in *Œuvres* ed. J.A. Serret, vol. VII, pp. 5–182. Paris: Gauthier-Villars, 1877; repr. Hildesheim, New York: Olms 1973.
- . 1775. Suite de recherches d'arithmétique. *Nouveaux Mémoires de l'Académie royale des Sciences et Belles-lettres de Berlin, année 1775* (1777), 323–356. Repr. in *Œuvres*, ed. J.-A Serret, vol. III, pp. 759–795. Paris: Gauthier-Villars, 1869; Hildesheim/New York: Georg Olms, 1973.
- LAM, Tsit-Yuen. 1973. *The Algebraic Theory of Quadratic Forms*. Reading: W.A. Benjamin. 2<sup>nd</sup> ed., 1980.
- LEGENDRE, Adrien-Marie. 1830. *Théorie des nombres*. 3<sup>rd</sup> ed. 2 vols. Paris: Didot.
- LEMMERMEYER, Franz. 2000. *Reciprocity Laws. From Euler to Eisenstein*. Berlin, Heidelberg, New York: Springer-Verlag.
- . 2007. *Reciprocity Laws. From Kummer to Hilbert*. In preparation.
- LEOPOLDT, Heinrich Wolfgang. 1953. Zur Geschlechtertheorie in abelschen Zahlkörpern. *Mathematische Nachrichten* 9, 351–362.
- MANIN, Yuri. 1972. *Kubicheskie formy: algebra, geometriya, aritmetika. (Cubic Forms: algebra, geometry, arithmetic.)* Moscow: Nauka. Engl. tr. M. Hazewinkel. Amsterdam: North-Holland, 1986.
- MANSION, Paul. 1896. Rapport. *Bulletin de l'Académie Royale des Sciences, des Lettres et des Beaux-Arts de Belgique* 3<sup>rd</sup> ser. 30, 189–193.
- NOETHER, Emmy. 1932. Hyperkomplexe Systeme in ihren Beziehungen zur kommutativen Algebra und zur Zahlentheorie. In *Verhandlungen des Internationalen Mathematiker-Kongresses Zürich 1932*, ed. W. Saxer, vol. I, pp. 189–194. Zürich: Orell-Füssli 1932. Repr. in *Gesammelte Abhandlungen – Collected Papers*, ed. N. Jacobson, pp. 636–641. Berlin, etc.: Springer, 1983.
- . 1933. Der Hauptgeschlechtssatz für relativ-galoissche Zahlkörper. *Mathematische Annalen* 108, 411–419. Repr. in *Gesammelte Abhandlungen – Collected Papers*, ed. N. Jacobson, pp. 670–678. Berlin, etc.: Springer, 1983.

- ONO, Takashi. 1985. A generalization of Gauss's theorem on the genera of quadratic forms. *Proceedings Japan Academy. Series A, Mathematical Sciences* 61, 109–111.
- RAZAR, Michael J. 1977. Central and genus class field and the Hasse norm theorem. *Compositio Mathematica* 35, 281–298.
- REICHARDT Hans. 1963. Über Dirichlet's zahlentheoretische Arbeiten. In *Bericht von der Dirichlet-Tagung*, ed. H. Reichardt, pp. 13–21. Berlin: Akademie-Verlag.
- SCHOLZ, Arnold. 1940. Totale Normenreste, die keine Normen sind, als Erzeuger nicht-abelscher Körpererweiterungen. 2. *Journal für die reine und angewandte Mathematik* 182, 217–234.
- SHANKS, Daniel. 1971a. Class number, a theory of factorization, and genera. In *1969 Number Theory Institute*, ed. D.J. Lewis, pp. 415–440. Proceedings of Symposia in Pure Mathematics 20. Providence: American Mathematical Society.
- . 1971b. Gauss's ternary form reduction and the 2-Sylow subgroup. *Mathematics of Computation* 25, 837–853; Corrigendum 32 (1978), 1328–1329.
- SHYR, Jih Min. 1975. On relative class numbers of certain quadratic extensions. *Bulletin of the American Mathematical Society* 81, 500–502.
- . 1979. Class numbers of binary quadratic forms over algebraic number fields. *Journal für die reine und angewandte Mathematik* 307/308, 353–364.
- SKOLEM, Thoralf. 1928. Geschlechter und Reziprozitätsgesetze. *Norsk matematisk Forenings skrifter* 1<sup>st</sup> ser. 18, 38pp.
- SKOROBOGATOV, Alexei. 2001. *Torsors and Rational Points*. Cambridge: Cambridge University Press.
- STARK, Harold M. 1976. The genus theory of number fields. *Communications on Pure and Applied Mathematics* 29, 805–811.
- STEINIG, John. 1966. On Euler's idoneal numbers. *Elemente der Mathematik* 21, 73–88.
- TANNAKA, Tadao. 1958. A generalized principal ideal theorem and a proof of a conjecture of Deuring. *Annals of Mathematics* 67, 574–589.
- TAUSSKY, Olga. 1983. Some non-commutative methods in algebraic number theory. In *Emmy Noether in Bryn Mawr*, ed. B. Srinivasan, J. Sally, pp. 47–57. New York, Berlin: Springer-Verlag.
- TERADA, Fumiuyuki. 1952. On the principal genus theorem concerning the Abelian extensions. *Tohoku Mathematical Journal* 4, 141–152.
- . 1953. A note on the principal genus theorem. *Tohoku Mathematical Journal* 5, 211–213.
- VENKOV, Boris Alekseevič. 1970. *Elementary Number Theory*. Transl. from Russian by H. Alderson. Groningen: Wolters-Noordhoff.
- WEBER, Heinrich. 1908. *Lehrbuch der Algebra*, vol. 3. Braunschweig: Vieweg. Repr. New York: Chelsea, 1961.
- WEIL, André. 1984. *Number Theory. An Approach through History from Hammurapi to Legendre*. Basel, Boston: Birkhäuser.
- ZAGIER, Don. 1981. *Zetafunktionen und quadratische Körper. Eine Einführung in die höhere Zahlentheorie*. Berlin, Heidelberg, New York: Springer-Verlag.