Ann. Sc. Math. Québec, 1979, Vol. III, No 1, pp. 5-62

ON THE DEVELOPMENT OF THE GENUS OF QUADRATIC FORMS

Günther Frei

A Peter Hilton, maître et ami.

RÉSUMÉ

La théorie du genre des formes quadratiques, des groupes nilpotents, des corps algébriques et encore d'autres concepts est essentiellement une théorie locale-globale qui a comme objectif l'étude de la question suivante: Dans quelle mesure des données locales déterminent-elles des objets globaux (principe de Hasse)? La notion du genre fut introduite par Gauss en 1801 mais ce fut Hasse qui en 1923 en reconnût son caractère local-global.

A l'origine du développement, on trouve un théorème de Fermat énoncé dans une lettre adressée à Mersenne (1640): un nombre premier impair p est la somme unique de deux carrés si et seulement si $p \equiv 1$ modulo 4 . La démonstration fut donnée par Euler, 114 ans plus tard, et Euler ainsi que Lagrange et Legendre trouvèrent d'autres théorèmes de ce type. Motivé par ces travaux sporadiques, Gauss en 1801, étudie d'une façon systématique la représentabilité d'un entier par une forme quadratique binaire quelconque à coefficients entiers. Dans ce but, Gauss ajoute aux théorèmes sur l'équivalence, sur les classes et sur le discriminant, déjà obtenus par Lagrange en 1773, les notions de genre et de composition des formes sur lesquelles il démontre des théorèmes de grande profondeur et d'une haute portée. La théorie des formes à 3 variables, initiée par Gauss et appliquée par lui-même au genre des formes binaires, est poursuivie par Seeber, et est étendue aux formes quadratiques à un nombre quelconque de variables par Eisenstein, Smith, Poincaré et Minkowski. Dans une annonce des travaux de Seeber, Gauss (1831) donne

aussi une interprétation géométrique de sa théorie des formes quadratiques binaires positives. Cette théorie est étendue aux formes quadratiques positives à un nombre quelconque de variables par Minkowski (1891). Elle conduit finalement à une théorie des formes quadratiques rationnelles en termes d'espaces quadratiques développés par Witt (1937), ainsi qu'à une théorie des formes quadratiques entières en termes de modules quadratiques développés systématiquement par Eichler (1952). Dans son livre, Eichler développe d'abord la théorie locale des complétés p-adiques des modules quadratiques afin d'obtenir des résultats globaux pour ceux-ci. Il obtient ainsi une théorie analogue mais beaucoup plus compliquée que la théorie rationnelle de Hasse, dans laquelle les nombres p-adiques, présentés par Hensel en 1899, sont appliqués pour la première fois avec grand succès, en leur assurant ainsi une place importante en mathématique. En s'appuyant sur l'interprétation du genre que donne Hasse en termes de nombres p-adiques, Kneser et Borel ont pu caractériser le genre d'une forme quadratique entière en termes d'adèles du groupe orthogonal associé. Cette caractérisation a préparé le chemin à l'étude du genre d'objets encore plus généraux, tels que par exemple le genre des groupes algébriques ou le genre des modules. Ce sont ces généralisations qui ont conduit à la définition du genre des groupes nilpotents donnée par Pickel et Mislin.

La théorie du genre de Gauss a encore joué un rôle très important dans un domaine très différent. Dedekind (1894) transposa la théorie de Gauss sur les formes quadratiques binaires de discriminant d en langage d'idéaux d'un corps quadratique de même discriminant. Les théorèmes fondamentaux de Gauss sur le genre, reformulés maintenant pour les corps quadratiques et généralisés aux corps de nombres cycliques de degré premier jouaient alors un rôle clé dans l'édification de la théorie des corps de classes par Hilbert, Takagi et Hasse. Plus tard (1951), Hasse donna une interprétation de la théorie du genre des corps quadratiques en termes de la théorie des corps de classes qui fut généralisée aux corps abéliens par Leopoldt (1953) et aux corps de nombres quelconques par Fröhlich (1959).

0. INTRODUCTION

Recently, P. Pickel [Pi-1971] and G. Mislin [Mis-1971] independently and Hilton-Mislin [H-M-1975] introduced the notion of a genus for nilpotent groups and P. Hilton gave an account of this theory within the fast growing theory of localization of nilpotent groups lately [Hi-1975] (see also [H-M-R-1975]). It might therefore be of some interest to trace back this notion of a genus to its origin and to look at some of its many interesting facets that developed during the last 175 years in fields closely related as quadratic forms, class field theory, algebraic groups and nilpotent groups.

1. THE GENUS OF QUADRATIC FORMS

1.1 Fermat [Fe-1640] stated in a letter to Mersenne that

Theorem 1.1. An odd prime number p is the sum of two (unique) squares (of positive integers), $p = x^2 + y^2$ $(x, y \in N)$ if and only if $p \equiv 1 \pmod{4}$.

The first proof of this theorem appeared more than a century later and was given by Euler [Eu-1754]. Whether or not p is decomposable into a sum of two squares depends therefore only on the congruence class of p modulo 4 .

1.2 Gauss in his fundamental treatise "Disquisitiones arithmeticae" [Ga-1801] solved completely the general problem:

What are the congruence conditions for an *integral binary quadratic form* $f = (a,b,c) = ax^2 + 2bxy + cy^2$ to represent an integer n , i.e., when does $ax^2 + 2bxy + cy^2 = n$ with integers a , b , c have integer solutions x , y .

He also found explicit formulae for the number of solutions in the case where the genus of f (see definition 2.5) contains only one equivalence class of forms (see below).

Let $T = (\alpha,\beta,\gamma,\delta)$ be the substitution $x = \alpha x' + \beta y'$, $y = \gamma x' + \delta y'$ where α , β , γ , δ are integers. Then

$$ax^2 + 2bxy + cy^2 = a'x'^2 + 2b'x'y' + c'y'^2$$

where $a' = a\alpha^2 + 2b\alpha\gamma + c\gamma^2$, $b' = a\alpha\beta + b(a\delta+b\gamma) + c\gamma\delta$, $c' = a\beta^2 + 2b\beta\delta + c\delta^2$. Gauss called the two forms $f = (a,b,c)$ and $f' = (a',b',c')$ *equivalent*, we shall write $f \simeq f'$, if the substitution $T = (\alpha,\beta,\gamma,\delta)$ satisfies $\alpha\delta - \beta\gamma = \pm 1$, and *properly equivalent*, we write $f \equiv f'$, if $\alpha\delta - \beta\gamma = +1$ [Ga-1801, Art. 157] .

In modern matrix notation (not yet employed by Gauss; it was only introduced by Sylvester and Cayley around 1855) this can be formulated in the following way. Associate to $f = (a,b,c)$ the symmetric integral square matrix $M_f = \begin{pmatrix} a & b \\ b & c \end{pmatrix}$ and to $T = (\alpha,\beta,\gamma,\delta)$ the integral square matrix $T = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$. If $T^t = \begin{pmatrix} \alpha & \gamma \\ \beta & \delta \end{pmatrix}$ denotes the transpose of T and $\det T = \alpha\delta - \beta\gamma$ the determinant of T then we have

Proposition 2.1. $f \simeq f'$ (respectively $f \equiv f'$) if and only if $M_{f'} = T^t M_f T$ with $\det T = \pm 1$ (respectively $\det T = +1$) .

We also note that if $X = \begin{pmatrix} x \\ y \end{pmatrix}$ then $ax^2 + 2bxy + cy^2 = X^t M_f X$. This yields immediately

Proposition 2.2. If $f \simeq f'$ then $\det M_f = \det M_{f'}$, and f and f' represent the same integers n .

One has only to note that the inverse of T is also an integer square matrix if $\det T = \pm 1$.

Gauss calls $d = b^2 - ac = -\det M_f$ the *determinant* of $f = (a,b,c)$ [Ga-1801, Art. 154] . He showed that the number of proper equivalence classes of forms with the same determinant is finite [Ga-1801, Art. 223] , a result that goes already back to Lagrange [Lag-1773] . The same holds true for equivalence classes, and more generally for equivalence classes of n-ary (see 1.5) quadratic forms (see [Eis-1847, p. 118-9] and also [Eic-1952, Satz 12.7]).

Next, Gauss considers the conditions for an integer n to be represented by the form f . He defines $f = (a,b,c)$ to be *primitive* if the greatest common divisor (g.c.d.) of a , b and c is one [Ga-1801, Art. 226] . Of course, if f is primitive and $f \simeq f'$ then also f' is primitive. The equivalence class of f is then said to be primitive also. The same applies to proper equivalence classes. Then Gauss proves the following remarkable property [Ga-1801, Art. 229] .

Theorem 2.3. Let $f = (a,b,c)$ be a primitive form and p a prime dividing the determinant: $p \mid d$, $d = b^2 - ac$. Let further denote by $f(Z^2) = \{m = ax^2 + 2bxy + cy^2 \mid (x,y) \in Z^2\}$ the set of integers represented by f .

Then the $m \in f(Z^2)$ not divisible by p are all either quadratic residues modulo p or quadratic non-residues modulo p .

Proof. Suppose that m , $m' \in f(Z^2)$ and that m and m' are not divisible by p , i.e. $m = ax^2 + 2bxy + cy^2$ and $m' = ax'^2 + 2bx'y' + cy'^2$ for some $x,y,x',y' \in Z$ and $p \nmid mm'$. Then

$$mm' = (axx' + b(xy'+yx') + cyy')^2 - d(xy' - yx')^2 .$$

Hence mm' is a quadratic residue modulo d and hence modulo p and m and m' are either both quadratic residues or quadratic non-residues modulo p .

Remark 2.4.

a) If $4 \mid d$ then the same argument shows that $mm' \equiv 1 \pmod 4$, i.e. the $m \in f(Z^2)$ are all either $\equiv 1 \pmod 4$ or $\equiv 3 \pmod 4$. If $8 \mid d$ then $mm' \equiv 1 \pmod 8$ and the $m \in f(Z^2)$ are all either $\equiv 1$ or $\equiv 3$ or $\equiv 5$ or $\equiv 7$ (mod 8) .

b) The odd primes not dividing the determinant do not furnish a characterization of the set $f(Z^2)$ but the two powers of the even prime $p = 2$, $4 = 2^2$ and $8 = 2^3$ do characterize it in the following way (see [Ga-1801, Art. 229]) : $f = (a,b,c)$ is still supposed to be primitive and $d = b^2 - ac$.

b1) If $d \equiv 3 \pmod 4$ then the odd $m \in f(Z^2)$ are all either $\equiv 1$ or $\equiv 3$ (mod 4) .

b2) If $d \equiv 2 \pmod 8$ then the odd $m \in f(Z^2)$ are all either $\equiv 1,7$ or $\equiv 3,5 \pmod 8$.

b3) If $d \equiv 6 \pmod 8$ then the odd $m \in f(Z^2)$ are all either $\equiv 1,3$ or $\equiv 5,7 \pmod 8$.

One verifies, still by the same argument, that in the case b1) one must have the condition $mm' \equiv 1 \pmod 4$ because of the hypothesis that m and m' are odd.

In case b2) one is led to the condition $mm' \equiv \pm 1 \pmod 8$ and in the case b3) to the condition $mm' \equiv 1,3 \pmod 8$.

The equivalence class (and hence also the proper equivalence class) of a primitive form f is therefore characterized by t odd *characters* (as Gauss called them) $\varepsilon_{p_1},\ldots,\varepsilon_{p_t}$, where t is the number of odd prime divisors of d, which indicate whether the $m \in f(Z^2)$ with $p_i \nmid m$ are quadratic residues modulo p_i $(i=1,\ldots,t)$ or not, and a character ε_2 related to the prime $p = 2$ (if $d \not\equiv 1$ modulo 4) which expresses a relation modulo 4 (if $d \equiv 0,3$ modulo 4) or modulo 8 (if $d \equiv 0,2,6$ modulo 8).

In Dirichlet's notation [Di-1839, §3] one puts $\varepsilon_{p_i}(f) = \left(\frac{m}{p_i}\right) = \left(\frac{a}{p_i}\right) = \left(\frac{c}{p_i}\right) = \pm 1$ for p_i odd and if $m \in f(Z^2)$ but p_i does not divide m, a and c, where $\left(\frac{\ }{p_i}\right)$ is the Legendre symbol[1]. Notice that not both a and c can be divisible by p_i if f is to be primitive, because of $p_i \mid (b^2 - ac)$, and that a and c are always represented by f.

[1] *i.e.* $\left(\frac{m}{p_i}\right) = +1$ *if* m *is a quadratic residue* mod p_i *and* $\left(\frac{m}{p_i}\right) = -1$ *if* m *is a non-residue.*

As far as the characters related to the prime 2 are concerned one puts $\varepsilon_2(f) = (-1)^{\frac{m-1}{2}}$ if $d \equiv 0,3,4,7 \pmod 8$, $= (-1)^{\frac{m^2-1}{2}}$ if $d \equiv 0,2 \pmod 8$ and $= (-1)^{\frac{m-1}{2}+\frac{m^2-1}{8}}$ if $d \equiv 6 \pmod 8$. Notice that in the case $d \equiv 0 \pmod 8$ we have split the character ε_2 which takes four values, into two characters $\varepsilon_{2_1}(f) = (-1)^{\frac{m-1}{2}}$ and $\varepsilon_{2_2}(f) = (-1)^{\frac{m^2-1}{8}}$ each taking on the two values ±1 independently.

Again m can be replaced by either a or c if we suppose that a and c are not both even. Gauss calls such a form *properly primitive* [Ga-1801, Art. 226]. Gauss also remarks [Ga-1801, Art. 225], that if the determinant d of a form $f = (a,b,c)$ is negative then a and c are both either positive or negative. In the first case f represents only non-negative numbers. f is then said to be *positive*. In the second case where a and c are both negative f represents non-positive numbers only. f is then called *negative*. For forms with negative determinant one has therefore an analogue to theorem 2.3 with respect to the absolute value sign.

For forms with negative determinant d we can hence put

$$\varepsilon_\infty(f) = \begin{cases} +1 & \text{if } f \text{ is positive} \\ -1 & \text{if } f \text{ is negative} \end{cases}$$

where ∞ is said to be the *infinite prime*.

We can now define Gauss' genus [Ga-1801, Art. 231].

Definition 2.5. Two properly primitive forms f_1 and f_2 of the same determinant d are in the same *genus*, in symbols $f_1 \sim f_2$, if $\varepsilon_p(f_1) = \varepsilon_p(f_2)$ for all odd primes p dividing d for $p = 2$ (if $d \not\equiv 1 \bmod 4$) and for $p = \infty$ (if $d < 0$).

$f_1 \equiv f_2$ implies $f_1 \simeq f_2$ which implies $f_1 \sim f_2$. Thus (the equivalence classes and) the proper equivalence classes of forms are distributed into at most

2^{t+s} genera, where t is the number of odd prime divisors of the determinant d and $s = 0,1,2$ depending on whether $d \equiv 1,5 \pmod 8$, $d \equiv 2,3,4,6,7 \pmod 8$, $d \equiv 0 \pmod 8$, and the number of equivalence classes as well as the number of proper equivalence classes in the same genus is therefore finite.

The form $f_0 = (1,0,-d)$ of determinant d is called the *principal form* its class the *principal class* and its genus the *principal genus*. Clearly one has $\varepsilon_p(f_0) = +1$ for all $p|d$, for $p = 2$ and $p = \infty$ so that the principal genus is characterized by the fact that all its characters are $+1$.

1.3 Let us recall that a primitive form $f = (a,b,c)$ is called *properly primitive* if a and c are not both even. All forms equivalent to a properly primitive form f are also properly primitive [Ga-1801, Art. 161] and the whole equivalence class of f is then said to be properly primitive. Gauss showed further that each non-empty genus contains the same number of properly primitive equivalence classes for a given determinant d [Ga-1801, Art. 252], that half of the possible character values in $\{\pm 1\}^{t+s}$ (where $s = 0,1,2$) correspond to an empty genus (those are determined by means of the reciprocity law [Ga-1801, Art. 263-4], which yields essentially one linear relation among the characters, explicitely $\prod_p \varepsilon_p(f) = +1$, where p runs through the odd primes $p|d$, 2 (if $d \not\equiv 1 \bmod 4$) and ∞ (if $d < 0$) (see Section 3.3, in particular Theorem 3.7)), and that the other half of the possible character values do correspond to non-empty properly primitive genera [Ga-1801, Art. 287]. To prove this last result Gauss initiates the theory of ternary quadratic forms.

1.4 The analogous study of *ternary integral quadratic forms* $f = \sum_{i,j=1}^{3} a_{ij}x_ix_j = f(x_1,x_2,x_3)$ to which one can associate the symmetric integral matrix $M_f = (a_{ij})$ (Gauss writes $\begin{pmatrix} a_{11} & a_{22} & a_{33} \\ a_{23} & a_{31} & a_{12} \end{pmatrix}$, see [Ga-1801, Art. 267]) is much more complicated, mainly because the set $f(Z^3)$ of integers represented by f is more difficult to describe. Eisenstein [Eis-1847] and Smith [Sm-1867-1] showed that $f(Z^3)$ not only depends on (quadratic residue) characters of the ternary form f but also on those of the *adjoint* ternary form F of f which corresponds to the adjoint matrix $\operatorname{adj} M_f = M_F$ of M_f.

Let f be a primitive ternary form (i.e. the g.c.d. of all the coefficients in M_f is one) and denote by Ω the greatest common divisor of the coefficients in the adjoint matrix M_F, i.e. Ω is the g.c.d. of the minor determinants of M_f. We put further $d = -\det M_f = -\Omega^2\Delta$ and $F = \Omega g$ where d is again the *determinant* of f [Ga-1801, Art. 267] and where g is said to be the *primitive adjoint* form of f. Notice that Δ is an integer and that $-\Omega\Delta^2$, $G = \Delta f$ and f are the determinant, the adjoint and the primitive adjoint form of g respectively, so that the relation between f and g is entirely reciprocal [Sm-1867-1, Art. 2] and [Eis-1847].

Two forms f and f' are again said to be in the same *genus* [Sm-1867-1, Art. 8] if they have the same characters (and same d and same Ω). Equivalent forms (defined as in proposition 2.1) have equivalent adjoint forms [Ga-1801, Art. 269] and hence the same Ω and Δ and the same characters, that is two equivalent forms belong to the same genus.

Smith now shows [Sm-1867-1, Art. 12]

Theorem 4.1. Two primitive ternary quadratic forms f and f' have the same determinant, the same invariants Ω and Δ and the same characters, i.e. f and f' are in the same genus, if and only if there exists a transformation $T = (t_{ij})$ with rational coefficients whose denominators are prime to $2\Omega\Delta$ and with determinant $\det T = 1$ such that $M_{f'} = T^tM_fT$.

Later, Speiser proved the analogous theorem for binary quadratic forms [Sp-1912].

1.5 Eisenstein, Smith, Poincaré and Minkowski arrived at similar criteria in the case of two *integral n-ary quadratic forms* f and f' thereby making use of all the *k-th adjoint* forms (Smith also uses the term comitant of the k-th species, see [Sm-1864]) of f. These are the quadratic forms corresponding to the k-th adjoint $(k=1,\dots,n-1)$ of the matrix $M_f = (a_{ij})$ belonging to the *integral n-ary quadratic form* $f = \sum_{i,j=1}^{n} a_{ij}x_ix_j$. The k-th adjoint or k-th derived matrix of M_f is the $\binom{n}{k}$-square matrix whose entries are the k-rowed minors of M_f . Poincaré [Po-1882] and Minkowski [Min-1886] define the genus in this general case as follows.

Definition 5.1. Two n-ary quadratic forms f and g lie in the same *genus*, in symbols $f \sim g$, if

(i) there exists a real matrix T such that $M_g = T^tM_fT$, i.e. f and g have the same Sylvester-index, in symbols $i(f) = i(g)$,

(ii) there exists for each integer m an integral matrix T_m such that $M_g \equiv T_m^tM_fT_m$ (modulo m) identically for all coefficients, and $\det T_m \equiv 1$ (modulo m).

Then Minkowski states [Min-1886].

Theorem 5.2. Two n-ary quadratic forms f and g belong to the same genus, $f \sim g$, if and only if

(i) $i(f) = i(g)$,

(ii) $\det M_f = \det M_g = d$,

(iii) $M_g \equiv T^tM_fT$ (mod 2d) and $\det T \equiv 1$ (mod 2d) for an integer matrix T .

This follows from a theorem of Smith [Sm-1867-2, p. 516] which generalizes theorem 4.1 to the case of n-ary quadratic forms. Smith [Sm-1867-2, Chap. 1] and Minkowski [Min-1884, Kap. XI] also describe the genera by means of characters similar to the cases $n = 2$ and 3 . For their work they were jointly awarded the Grand Prix of the French Academy in Paris in 1884.

The definition 5.1 of the genus by Poincaré and Minkowski involves infinitely many conditions, namely congruence conditions modulo all prime powers p^s for all primes p . By virtue of theorem 5.2 only finitely many conditions are essentially needed, namely the congruence conditions modulo the prime powers dividing $2d$.

Moreover one can dispense with the condition $\det T_m \equiv 1 \pmod{m}$ by virtue of the following:

Proposition 5.3. If f and g are two quadratic forms with matrices M_f and M_g and with the same determinant $\det M_f = \det M_g = d$ such that for every prime power p^s there exists an integer matrix T with $M_g \equiv T^tM_fT \pmod{p^s}$ then there exists an integer matrix T_0 satisfying $M_g \equiv T_0^tM_fT_0 \pmod{p^s}$ and $\det T_0 \equiv 1 \pmod{p^s}$ for all prime powers p^s .

Proof. Let p^r be the highest power of p dividing $2d$. By hypothesis there exists an integer matrix T_1 so that $M_g \equiv T_1^tM_fT_1 \pmod{p^{r+s}}$ for any $s \in N$. Taking determinants we get $d \equiv (\det T_1)^2 d \pmod{p^{r+s}}$, hence $d(\det T_1-1)(\det T_1+1) \equiv 0 \pmod{p^{r+s}}$ and therefore $\det T_1 \equiv \pm 1 \pmod{p^s}$. If $\det T_1 \equiv 1 \pmod{p^s}$ we put $T_1 = T_0$ and we are done. In the opposite case, we use the fact that there always exists an integer matrix A such that $M_f \equiv A^tM_fA \pmod{p^s}$ and $\det \equiv -1 \pmod{p^s}$ for any prime power p^s and any n-ary quadratic form f . This last fact is easily verified for the standard form $f' = x_1^2 + \dots + x_{n-1}^2 + ax_n^2$ (where a is either one if d is a square, or a non-square modulo p^s if d is not a square). Simply take $A : x_1 \to -x_1$, $x_i \to x_i$ for $i = 2,\dots,n$. If f is any other n-ary form, then f is equivalent to such a standard form f' modulo p^s [Se-1973, prop. 5, Chap. IV, 1], i.e. there exists an integral matrix B with $M_{f'} \equiv B^tM_fB \pmod{p^s}$. We remark that B is invertible modulo p^s , hence $\det B$ is a unit modulo p^s and therefore p does not divide $\det B = b$. If C is an integral matrix with $M_{f'} \equiv C^tM_{f'}C \pmod{p^s}$ and $\det C \equiv -1 \pmod{p^s}$ then we take $A = BC(aqB^{-1})$ where q is chosen such that qB^{-1} is an integral matrix and q is prime to p (we can take for example $q = b = \det B$) and a is a number with the property that $aq \equiv 1 \pmod{p^s}$. Then A has the required properties with respect to f and we can put $T_0 = T_1A$.

The genus can now be characterized in the following way:

Theorem 5.4. Two n-ary quadratic forms f and g belong to the same genus if and only if

(i) $i(f) = i(g)$, i.e. there exists a real matrix T such that $M_g = T^t M_f T$,

(ii) for every prime p and every prime power p^s there exists an integral matrix T_{p^s} such that $M_g \equiv T^t_{p^s} M_f T_{p^s}$ (modulo p^s) .

1.6 Hensel [Hen-1913] in the case $n = 2$ and 3 and Hasse [Ha-1923-1-2] in the general case applied the p-adic numbers introduced by Hensel [Hen-1913] to quadratic forms, whereby Hasse discovered the *local-global-principle* (which says that a property holds in Q if and only if it holds in all $\hat{Q}_{(p)}$ for all primes p and for $p = \infty$, see below) first for the representability of a rational number by a rational quadratic form [Ha-1923-1] and then for the rational equivalence of two rational quadratic forms [Ha-1923-2], a principle which turned out to be very important in number theory.

Hensel called a rational number $r = \frac{a}{b}$ $(a,b \in Z)$ *locally integral* at the prime number p , if p does not divide b , and he said that $r = \frac{a}{b}$ is a *local unit* if $r = \frac{a}{b}$ and $\frac{1}{r} = \frac{b}{a}$ are locally integral at p , i.e. if p does not divide a nor b .

The *p-adic numbers* $\hat{Q}_{(p)}$, where p is an integer prime number, consists of the set of formal power series in p with rational coefficients which are locally integral at p and with only finitely many terms of negative exponent: $\hat{Q}_{(p)} = \{a_{-s}p^{-s} + \ldots + a_{-1}p^{-1} + a_0 + a_1p + a_2p^2 + \ldots \mid a_i = \frac{b_i}{c_i} \in Q$ and $p \nmid c_i\}$. Two p-adic numbers as formal power series in p are said to be equal if they are congruent modulo all powers of p . If for example (a) and (b) are p-adic numbers, i.e. $(a) = \sum\limits_{n=-s}^{\infty} a_np^n$ and $(b) = \sum\limits_{n=-s}^{\infty} b_np^n$ (some or all of the coefficients can be zero) and $(a)_k$ and $(b)_k$ are their approximations modulo p^{k+1} , i.e. $(a)_k = a_{-s}p^{-s} + \ldots + a_kp^k$ and $(b)_k = b_{-s}p^{-s} + \ldots + b_kp^k$ then $(a) = (b)$ if and only if $(a)_k \equiv (b)_k \pmod{p^{k+1}}$ for all $k \in N$.

In $\hat{Q}_{(p)}$ one defines an addition and a multiplication which is ordinary addition and multiplication of power series and also ordinary addition and multiplication modulo all powers of p . If for example $(a) = a_{-s}p^{-s} + \ldots + a_0 + a_1p + \ldots$, $(b) = b_{-s}p^{-s} + \ldots + b_0 + b_1p + \ldots \in \hat{Q}_{(p)}$ then

$$(a) + (b) = (c) = (a_{-s}+b_{-s})p^{-s} + \ldots + (a_0+b_0) + (a_1+b_1)p + \ldots$$

and

$$(a) \cdot (b) = (d) = (a_{-s}b_{-s})p^{-2s} + \ldots + (a_{-s}b_s + a_{-s+1}b_{s-1} + \ldots + a_0b_0 + \ldots + a_sb_{-s}) + (a_{-s}b_{s+1} + \ldots + a_{s+1}b_{-s})p + \ldots$$

are their p-adic sum and product respectively and one verifies that $(c)_k \equiv (a)_k + (b)_k \pmod{p^{k+1}}$ and $(d)_k \equiv (a)_k \cdot (b)_k \pmod{p^{k+1}}$ for all k .

The coefficients $\overline{a}_i$ in the p-adic development of a p-adic number (a) can be so determined that $0 \le \overline{a}_i < p$ with $\overline{a}_i \in Z$. We then call $(a) = \overline{a}_{-s}p^{-s} + \ldots + \overline{a}_0 + \overline{a}_1p + \ldots$ the *reduced representation* or the *reduced development* of (a) .

Every p-adic number (a) admits a unique reduced representation, i.e. its reduced coefficients $\overline{a}_i$ $(0 \le \overline{a}_i < p)$, $\overline{a}_i \in Z$ are uniquely determined and they can be found successively by congruence relations modulo all powers of p .

The formal power series $(a) = a_{-s}p^{-s} + \ldots + a_0 + a_1p + \ldots$ is not convergent in the ordinary sense (absolute value topology) but in the p-adic sense (p-adic topology) which expresses simply the fact that a p-adic number indicates a congruence behaviour modulo all powers of p . If $(a) = \overline{a}_rp^r + \ldots$ is a p-adic number given by its reduced representation, i.e. if p^r is the highest power of p dividing (a) then the p-adic value $|\ |_p$ of (a) is $|(a)|_p = \frac{1}{p^r}$, so that the p-adic value of (a) is small if (a) is divisible by a high power of p. Two numbers (a) and (b) are close in the p-adic topology if the p-adic value of their difference is small, that is if they are congruent modulo a high power of p.

The subring of $\hat{Q}_{(p)}$ of all formal power series with no coefficients of negative index is called the ring of *p-adic integers* and is denoted by $\hat{Z}_{(p)} = \{a_0 + a_1 p + \ldots + a_r p^r + \ldots \mid a_i = \frac{b_i}{c_i} \in Q, p \nmid c_i\}$. The multiplicative subgroup of $\hat{Z}_{(p)}$ of elements whose constant coefficient a_0 is not divisible by p is called the group of *p-adic units* and shall be denoted by $\hat{U}_{(p)} = \{a_0 + a_1 p + \ldots + a_n p^n + \ldots \mid a_i = \frac{b_i}{c_i} \in Q, p \nmid c_i, a_0 \text{ a local unit}\}$. It is the group of invertible elements in $\hat{Z}_{(p)}$.

All rational numbers of the form $\frac{a}{p^n}$, where a and n are natural numbers and p is a fixed prime, belong to $\hat{Q}_{(p)}$ and they are characterized by the fact that their p-adic development is finite. But also all negative and all rational numbers belong to $\hat{Q}_{(p)}$ as every rational number admits a unique reduced p-adic development. The reduced 7-adic development of $\frac{1}{3}$, for instance, can be found in the following manner. Put $\frac{1}{3} = a_0 + a_1 7 + a_2 7^2 + \ldots$ and determine the coefficients a_i successively modulo all powers of 7, i.e. $3a_0 \equiv 1 \pmod 7$ hence $a_0 = 5$, $3 \cdot 5 + 3 \cdot a_1 7 \equiv 1 \pmod{7^2}$ hence $2 + 3a_1 \equiv 0 \pmod 7$ and therefore $a_1 = 4$, $3 \cdot 5 + 3 \cdot 4 \cdot 7 + 3a_2 7^2 \equiv 1 \pmod{7^3}$ implies $2 + 3a_2 \equiv 0 \pmod 7$ thus $a_2 = 4$, and so on, and we get $\frac{1}{3} = 5 + 4 \cdot 7 + 4 \cdot 7^2 + \ldots$ [1].

Q is therefore contained in $\hat{Q}_{(p)}$ for all primes p in much the same way as Q is contained in the real numbers $\mathbb{R}$ which are often denoted by $\hat{Q}_{(\infty)}$. In brief, $\hat{Q}_{(p)}$ is the completion of Q with respect to the p-adic topology in the same way as $\mathbb{R} = \hat{Q}_{(\infty)}$ is the completion of Q with respect to the ordinary absolute value topology. We just mention *en passant* that $\hat{Q}_{(p)}$ is locally compact and that $\hat{Z}_{(p)}$ and $\hat{U}_{(p)}$ are compact subgroups of $\hat{Q}_{(p)}$ with respect to the p-adic topology.

[1] *Another (non-reduced) development of* $\frac{1}{3}$ *is the following "geometric series"* $\frac{1}{3} = \frac{2}{6} = \frac{-2}{-6} = -2 = \frac{1}{1-7} = -2(1+7+7^2+\ldots) = -2 - 2 \cdot 7 - 2 \cdot 7^2 - \ldots$

In the language of p-adic numbers the following defintion of the genus can now be given

Definition 6.1. Two n-ary quadratic forms $f = \sum_{i,j=1}^{n} a_{ij}x_i x_j$ and $g = \sum_{i,j=1}^{n} b_{ij}x_i x_j$ with associated symmetric matrices $M_f = (a_{ij})$ and $M_g = (b_{ij})$ are in the same *genus*, $f \sim g$, if

(i) $M_g = T^t M_f T$ for a real invertible matrix T;

(ii) $M_g = T_p^t M_f T_p$ for an integrally invertible matrix T_p with integer p-adic coefficients for all primes p.

1.7 In connection with the reduction theory of quadratic n-ary forms Minkowski [Min-1891] associates with a positive (definite) quadratic form $f = \sum_{i,j=1}^{n} a_{ij}x_i x_j$ a lattice L_f in $\mathbb{R}^n$ in the following way, an idea that already goes back to Gauss [Ga-1831] in the case of binary and ternary positive quadratic forms.

As f is a positive definite form there exists an (invertible) substitution T with real coefficients such that

$$f(x) = f(x_1,\ldots,x_n) = \sum_{i,j=1}^{n} a_{ij}x_i x_j = x_1'^2 + \ldots + x_n'^2 = f'(x_1',\ldots,x_n') = f'(x')$$

where $x = Tx'$ and where $x = (x_1,\ldots,x_n)$, $x' = (x_1',\ldots,x_n')$. In other words the matrix M_f can be diagonalized orthonormally over $\mathbb{R}$, $I_n = M_{f'} = T^t M_f T$ where I_n is the unit n-square matrix. Interprete now $f'(x')$ as being the euclidean metric in the real vector space $\mathbb{R}^n$ with the natural base $e_1 = (1,0,\ldots,0)$, $\ldots$, $e_n = (0,\ldots,0,1)$. Put $T^{-1}e_i = b_i \in R^n$ for $i = 1,\ldots,n$ and $L_f = \{x_1 b_1 + \ldots + x_n b_n \mid x_i \in Z\}$. L_f is called the *lattice* in $\mathbb{R}^n$

associated with the positive definite form f. It is unique up to equivalence (see definition 11.1) that is up to an orthogonal transformation, and one has $<b_i,b_j> = a_{ij}$, where $< , >$ stands for the ordinary scalar product (euclidean metric) in $\mathbb{R}^n$. Moreover

$$f(x_1,\dots,x_n) = \sum_{i,j=1}^{n} a_{ij}x_ix_j = \sum_{i,j=1}^{n} <b_i,b_j>x_ix_j = <x_1b_1+\dots+x_nb_n, x_1b_1+\dots+x_nb_n> .$$

The base $b_1,\dots,b_n$ of L_f spans a n-parallelohedron $P = \mathbb{R}^n/L_f$ of volume $\mathrm{vol}\ P = (\det M_f)^{\frac{1}{2}} = \det T^{-1} = \frac{1}{\det T}$.

1.8 Witt [Wi-1937] considers generally any n-ary quadratic form

$$f = f(x) = f(x_1,\dots,x_n) = \sum_{i,j=1}^{n} a_{ij}x_ix_j$$

over a field k (i.e. $a_{ij} \in k$) of characteristic not 2 as being a (generalized) metric over the vector space k^n, and he calls the pair (k,f) or (k^n,f) a *metric vector space* over k. If $b_1,\dots,b_n$ is any basis over k^n he defines $(b_i,b_j)_f = a_{ij}$, where $(,)_f$ denotes the symmetric bilinear form (inner product) associated with f, i.e. $(x_1b_1+\dots+x_nb_n, y_1b_1+\dots+y_nb_n)_f = \frac{1}{2}[f(x_1+y_1,\dots,x_n+y_n) - f(x_1,\dots,x_n) - f(y_1,\dots,y_n)]$. A change of basis $c_i = Tb_i$ $(i = 1,\dots,n)$ corresponds to taking an equivalent form $f' = \sum_{i,j=1}^{n} a'_{ij}x'_ix'_j$ as follows. If $v = x_1b_1+\dots+x_nb_n = x'_1c_1+\dots+x'_nc_n$ is an arbitrary vector represented with respect to the two bases $b_1,\dots,b_n$ and $c_1,\dots,c_n$ and $c_i = Tb_i$ is a change of basis from the b_i to the c_i, i.e. $c_i = \sum_{j=1}^{n} t_{ji}b_j$, where $T = (t_{ij}) = (t_{ji})^t$, then $X = TX'$ where $X = (x_1,\dots,x_n)^t$ and $X' = (x'_1,\dots,x'_n)^t$ are the coordinates of v with respect to the b_i and c_i.

We require now that

$$(v,v)_f = f(v) = f(x) = \sum_{i,j=1}^{n} (b_i,b_j)_f x_ix_j = \sum_{i,j=1}^{n} (c_i,c_j)_{f'} x'_ix'_j$$
$$= f'(x') = f'(v) = (v,v)_{f'}$$

and this condition yields $M_{f'} = T^tM_fT$ where $M_f = ((b_i,b_j)_f) = (a_{ij})$ and $M_{f'} = ((c_i,c_j)_{f'}) = (a'_{ij})$ so that f' is *equivalent* to f over k (which means that the coefficients of the transformation matrix $T = (t_{ij})$ lie in k).

Conversely, equivalent forms f and f' over k, i.e. those satisfying $M_{f'} = T^tM_fT$ for an invertible matrix $T = (t_{ij})$ with coefficients in k, correspond to the same metric space with respect to two different bases $b_1,\dots,b_n$ and $c_1,\dots,c_n$ where $c_i = \sum_{j=1}^{n} t_{ji}b_j$. Furthermore $\det M_{f'} = \det M_f (\det T)^2$.

1.9 The group of automorphisms of k^n preserving the metric f in the vector space k^n is called the *orthogonal group* of (k^n,f) associated with f. We shall denote it by $O_f = \{T \in \mathrm{Aut}(k^n,f) \mid f(Tv) = f(v) \text{ for all } v \in k^n\}$.

We can suppose that $b_1,\dots,b_n$ is the natural basis of (k^n,f). Then $v = x_1b_1+\dots+x_nb_n = (x_1,\dots,x_n) = x$ and $O_f = \{T \in GL(n,k) \mid T^tM_fT = M_f\}$. We keep in mind that $\det T = \pm 1$ if $T \in O_f$. T is called *proper* if $\det T = +1$.

1.10 The definitions and notations of 1.8 and 1.9 can be extended to the case where k is a (commutative unitary) ring of characteristic not 2. (k^n,f) is then said to be a *metric module* of dimension n. If T is a change of basis then $\det T$ has to be a unit in k, as T^{-1} is also a matrix over k. We shall call such a matrix *unimodular*.

1.11 Following Eichler [Eic-1952] the theory of integral quadratic forms (over the integers of an algebraic number field) k, in which every ideal is a principal ideal, can be translated into the language of lattices in the following way[1] .

[1] *The general case of any algebraic number field also treated by Eichler is much more complicated.*

Let $V = (k^n, f)$ be a metric vector space over the algebraic number field k with respect to the quadratic form $f = \sum_{i,j=1}^{n} a_{ij}x_ix_j$ over k and let $b_1,\ldots,b_n$ be the natural basis of k^n. Denote by $\underset{\sim}{g}$ the integers in k [1]. $\underset{\sim}{g}^n = \{x_1b_1+\ldots+x_nb_n \mid x_i \in \underset{\sim}{g}\}$ is a lattice in k^n. In general we call any module $L = \{x_1d_1+\ldots+x_nd_n \mid x_i \in \underset{\sim}{g}$, where $d_1,\ldots,d_n$ is a basis of $k^n\} = [d_1,\ldots,d_n]$ a *lattice* in k^n.

Definition 11.1. Two lattices $L = [d_1,\ldots,d_n]$ and $K = [c_1,\ldots,c_n]$ in k^n are called equivalent, in symbols $L \simeq K$, if there exists an orthogonal transformation $S \in 0_f$ such that $L = SK$.

Similarly, the two lattices L and K are called *properly equivalent*, in symbols $L \equiv K$, if there exists a proper orthogonal transformation $S \in 0_f^+ = \{S \in 0_f \mid \det S = +1\}$ such that $L = SK$.

One can associate with $L = [d_1,\ldots,d_n]$ the matrix $M_L = ((d_i,d_j)_f)$ and with $K = [c_1,\ldots,c_n]$ the matrix $M_K = ((c_i,c_j)_f)$. Of course, $M_{\underset{\sim}{g}^n} = ((b_i,b_j)_f) = (a_{ij}) = M_f$. The matrices M_L and M_K determine (rational) quadratic forms f_L and f_K with coefficients in k (in the sense of 1.2 or 1.5). Clearly $M_{\underset{\sim}{g}^n}$ determines f.

Definition 11.2. f_L is defined to be *equivalent* to f_K (over $\underset{\sim}{g}$), in symbols $f_L \simeq f_K$, if there exists an integral unimodular matrix T (i.e. with coefficients in $\underset{\sim}{g}$ and with $\det T$ a unit in $\underset{\sim}{g}$) such that $M_K = T^tM_LT$.

Similarly, f_L is *properly equivalent* to f_K (over $\underset{\sim}{g}$), we write $f_L \equiv f_K$, if there exists a proper integral unimodular matrix T (whose determinant is a positive unit in $\underset{\sim}{g}$) such that $M_K = T^tM_LT$.

[1] *The coefficients* a_{ij} *may lie in* k, *but we are concerned with the case where the indeterminates* x_i *and* x_j *take values in* $\underset{\sim}{g}$.

This definition is in accordance with 1.8 and 1.10 and generalizes the definition in 1.2 where $k = Q$, $\underset{\sim}{g} = Z$ and $n = 2$. Clearly f_L does not depend on the basis $b_1,\ldots,b_n$ chosen for f, but it does depend on the basis $d_1,\ldots,d_n$ of L. However, it follows from 1.8 and 1.10 that the equivalence class of f_L is independent of the basis $d_1,\ldots,d_n$ chosen for L. More generally we have

Proposition 11.3. $L \simeq K$ if and only if $f_L \simeq f_K$. Similarly, $L \equiv K$ if and only if $f_L \equiv f_K$. In particular $L \simeq (\equiv)\underset{\sim}{g}^n$ if and only if $f_L \simeq (\equiv)f$.

Proof. Let $L = [d_1,\ldots,d_n]$, $K = [c_1,\ldots,c_n]$, $M_L = ((d_i,d_j)_f)$, $M_K = ((c_i,c_j)_f)$. If $L \simeq K$ then there exists an orthogonal transformation $S \in 0_f$ so that $L = SK$. Put $Sc_i = t_{1i}d_1+\ldots+t_{ni}d_n$ and $T = (t_{ki})$. $Sc_1,\ldots,Sc_n$ is a basis of L as well as $d_1,\ldots,d_n$. Hence T must be integral and integrally invertible hence unimodular. Furthermore

$$(c_i,c_j)_f = (Sc_i,Sc_j)_f = \left(\sum_{k=1}^{n} t_{ki}d_k, \sum_{\ell=1}^{n} t_{\ell j}d_\ell\right)_f = \sum_{k=1}^{n}\sum_{\ell=1}^{n} t_{ki}(d_k,d_\ell)_f\, t_{\ell j}$$

hence $M_K = T^tM_LT$.

Conversely, suppose that $M_K = T^tM_LT$ for an integral unimodular matrix T. Then the linear transformation S defined by $Sc_i = \sum_{k=1}^{n} t_{ki}d_k$ is well determined and

$$(c_i,c_j)_f = \sum_{k=1}^{n}\sum_{\ell=1}^{n} t_{ki}(d_k,d_\ell)_f\, t_{\ell j} = \left(\sum_{k=1}^{n} t_{ki}d_k, \sum_{\ell=1}^{n} t_{\ell j}d_\ell\right)_f = (Sc_i,Sc_j),$$

Hence $S \in 0_f$.

The proof for proper equivalence runs similarly.

We call again $f(L) = \{f(x) \mid x \in L\}$ the set of (algebraic) numbers represented by L and $\det M_L$ the determinant of L.

Equivalent lattices, $L \simeq K$, represent the same numbers, $f(L) = f(K)$ and have the same determinant up to a square of a unit. In particular

$f(L) = f_L(\sigma^n)$ if $L \simeq \mathfrak{o}^n$.

If $\mathfrak{p} \subseteq \mathfrak{o}$ is a prime ideal in $\mathfrak{o}$ then $\hat{k}_\mathfrak{p}$ stands for the $\mathfrak{p}$-adic numbers over k ($\mathfrak{p}$-adic completion of k) with respect to $\mathfrak{p}$. Again $\hat{k}_\mathfrak{p}$ can be defined as the field of formal power series $(\alpha) = \alpha_{-s}\pi^{-s} + \dots + \alpha_{-1}\pi^{-1} + \alpha_0 + \alpha_1 + \dots$ in a so called uniformizing element π lying in $\mathfrak{p}$ but not in $\mathfrak{p}^2$ and where the coefficients are locally integral at $\mathfrak{p}$, that is $\alpha_i = \frac{\beta_i}{\gamma_i}$ with integers β_i and $\gamma_i \in \mathfrak{o}$ and $\mathfrak{p}$ not dividing γ_i . One can easily show that $\hat{k}_\mathfrak{p}$ thus defined does not depend upon the chosen uniformizing parameter $\pi \in \mathfrak{p} - \mathfrak{p}^2$ (see for instance [Wey-1940]). The $\mathfrak{p}$-adic integers $\hat{\mathfrak{o}}_\mathfrak{p}$ and the unit group $\hat{U}_\mathfrak{p}$ are defined in the same way as for $k = Q$ and one has, of course, that $\hat{k}_\mathfrak{p} = \hat{Q}_{(p)}$, $\hat{\mathfrak{o}}_\mathfrak{p} = \hat{Z}_{(p)}$ and $\hat{U}_\mathfrak{p} = \hat{U}_{(p)}$ if $k = Q$ and $\mathfrak{p} = (p)$, where (p) is the ideal generated by the prime number p .

We remark that Hensel introduced the $\mathfrak{p}$-adic numbers for algebraic number fields as analoga of Puiseux-series already 1899 in a short notice in Jahresbericht der Deut. Math. Ver. Bd. 6, 83-88.

If $L = \mathfrak{o}a_1 + \dots + \mathfrak{o}a_n = [a_1,\dots,a_n]$ with $a_i \in k^n$ $(i = 1,\dots,n)$ is a lattice in k^n then we denote by $\hat{L}_\mathfrak{p} = \hat{\mathfrak{o}}_\mathfrak{p}a_1 + \dots + \hat{\mathfrak{o}}_\mathfrak{p}a_n = \hat{\mathfrak{o}}_\mathfrak{p}L$ the *$\mathfrak{p}$-adic extension* of L which is a so called local lattice in $\hat{k}^n_\mathfrak{p}$. One has (see [Eic-1952, Satz 12.1])

Proposition 11.4. $L = [a_1,\dots,a_n]$ is the intersection $L = k^n \cap \hat{L}_{\mathfrak{p}_1} \cap \hat{L}_{\mathfrak{p}_2} \cap \dots$ of k^n and of all local lattices $\hat{L}_\mathfrak{p}$, and $\hat{L}_\mathfrak{p} = \hat{\mathfrak{o}}^n_\mathfrak{p}$ for almost all prime ideals $\mathfrak{p}$ (the exceptions being the prime ideals dividing the denominators of the components of $a_1,\dots,a_n$ and those prime ideals dividing at the same time all the numerators of the ν-th components $a_{1\nu},\dots,a_{n\nu}$ of the basis $a_1,\dots,a_n$ of L ; the components taken with respect to the natural basis $b_1,\dots,b_n$ of k^n or of $\hat{k}^n_\mathfrak{p}$) .

Conversely, if the $\hat{L}_\mathfrak{p}$ are (local) lattices in $\hat{k}^n_\mathfrak{p}$ so that $\hat{L}_\mathfrak{p} = \hat{\mathfrak{o}}^n_\mathfrak{p}$ for almost all prime ideals $\mathfrak{p}$ then $L = k^n \cap \hat{L}_{\mathfrak{p}_1} \cap \hat{L}_{\mathfrak{p}_2} \cap \dots$ is a unique (global) lattice in k^n with the property $\hat{\mathfrak{o}}_\mathfrak{p}L = \hat{L}_\mathfrak{p}$.

Definition 11.5. Two lattices L and K in (k^n,f) belong to the same *genus*, in symbols $L \sim K$, if $\hat{L}_\mathfrak{p} \simeq \hat{K}_\mathfrak{p}$ for all $\mathfrak{p}$, i.e. if there exists for each prime ideal $\mathfrak{p}$ a (local) orthogonal transformation $S_\mathfrak{p} \in O_{f\mathfrak{p}} = \{$automorphisms of $(\hat{k}^n_\mathfrak{p},f) \mid f(S_\mathfrak{p}v) = f(v)$ for all $v \in \hat{k}^n_\mathfrak{p}\}$ such that $\hat{L}_\mathfrak{p} = S_\mathfrak{p}\hat{K}_\mathfrak{p}$.

We note that $L \sim K$, i.e. $\hat{L}_\mathfrak{p} = S_\mathfrak{p}\hat{K}_\mathfrak{p}$ for all $\mathfrak{p}$ and $\hat{K}_\mathfrak{p} = \hat{\mathfrak{o}}^n_\mathfrak{p}$ and $\hat{L}_\mathfrak{p} = \hat{\mathfrak{o}}^n_\mathfrak{p}$ for almost all $\mathfrak{p}$ implies that $S_\mathfrak{p} \in GL(n,\mathfrak{o}_\mathfrak{p})$ for almost all $\mathfrak{p}$.

If we generalize the definition 6.1 to algebraic number fields as follows

Definition 11.6. Two quadratic forms f_L and f_K over $\mathfrak{o}$ are in the same *genus*, we write $f_L \sim f_K$, if f_L and f_K are equivalent over all local integers $\hat{\mathfrak{o}}_\mathfrak{p}$, which means that $M_K = T^t_\mathfrak{p}M_LT_\mathfrak{p}$ for an integrally invertible matrix $T_\mathfrak{p}$ with integer $\mathfrak{p}$-adic coefficients (in $\hat{\mathfrak{o}}_\mathfrak{p}$) for all prime ideals $\mathfrak{p}$, then we get the following characterization of a genus.

Proposition 11.7. $L \sim K$ if and only if $f_L \sim f_K$.

In particular $L \sim \mathfrak{o}^n$ if and only if $f_L \sim f$.

The proof that $\hat{L}_\mathfrak{p} \simeq \hat{K}_\mathfrak{p}$ if and only if $f_{\hat{L}_\mathfrak{p}} \simeq f_{\hat{K}_\mathfrak{p}}$ over $\hat{\mathfrak{o}}_\mathfrak{p}$ for a prime ideal $\mathfrak{p}$ is similar to the proof of proposition 11.3.

1.12 Chevalley [Ch-1936] introduced the (multiplicative) *idèles* in connection with the multiplicative class field theory [Ch-1940] and Artin-Whaples [A-W-1945] introduced the additive *adèles* (or valuation vectors as they called them). The adèles $A = A_Q$ over Q can be defined in the following way.

Let $\hat{Q}_{(p)}$ stand for the p-adic numbers and $\hat{Z}_{(p)}$ for the p-adic integers, then $\hat{Q}_{(p)} = Q + \hat{Z}_{(p)}$. We put $\hat{Q}_{(\infty)} = \hat{Z}_{(\infty)} = \mathbb{R}$ the real numbers.

Definition 12.1. $A = A_Q = \{(a_\infty, a_2, a_3, a_5, \ldots, a_p, \ldots) \mid a_p \in \hat{Q}_{(p)}$ for all places $p = \infty, 2, 3, 5, \ldots$ and $a_p \in \hat{Z}_{(p)}$ for almost all $p\}$ are called the *adèles* of Q .

Addition and multiplication in A is defined component-wise.

Definition 12.2. $A^\infty = A_Q^\infty = R \times \hat{Z}_{(2)} \times \hat{Z}_{(3)} \times \hat{Z}_{(5)} \times \ldots \times \hat{Z}_{(p)} \times \ldots \subset A$.

Q can be imbedded into A in the following way. We view $a \in Q$ as a p-adic number in $\hat{Q}_{(p)}$ for all primes p and as a real number in $\hat{Q}_{(\infty)} = \mathbb{R}$. Then $\rho(a) = (a,a,a,\ldots,a,\ldots)$ is an adèle called a *principal adèle.* We identify Q with the field of principal adèles $\rho(Q) \subset A$.

$Q = \rho(Q)$ is discrete in A and A is locally compact (with respect to the product topology, where the p-adic topology is taken in $\hat{Q}_{(p)}$) . Furthermore

$$A = (\mathbb{R}\times\hat{Z}_{(2)}\times\hat{Z}_{(3)}\times\hat{Z}_{(5)}\times\ldots\times\hat{Z}_{(p)}\times\ldots) + Q = ([0,1)\times\hat{Z}_{(2)}\times\hat{Z}_{(3)}\times\ldots\times\hat{Z}_{(p)}\times\ldots) \oplus Q$$

where $\oplus$ denotes the direct sum and $[0,1) = \{x \in \mathbb{R} \mid 0 \le x < 1\}$
$A/Q \simeq [0,1) \times \hat{Z}_{(2)} \times \hat{Z}_{(3)} \times \hat{Z}_{(5)} \times \ldots \times \hat{Z}_{(p)} \times \ldots = F$ is called the *fundamental domain* of A .

The idèles $I_Q = I$ are the units in A . They can also be defined as follows.

Definition 12.3. $I = \{(a_\infty, a_2, a_3, a_5, \ldots, a_p, \ldots)$ $a_p \in \hat{Q}_{(p)}$ for all places $p = \infty, 2, 3, 5, \ldots$ and $a_p \in \hat{U}_{(p)} = \hat{Z}_{(p)} - p\hat{Z}_{(p)}$ = units in $\hat{Q}_{(p)}$, for almost all $p\}$.

1.13 Weil [Wei-1961] generalized the notion of adèles to arbitrary linear algebraic groups over Q , i.e. to Zariski closed subgroups of GL(n,Q) . These are groups of rational n × n matrices satisfying certain algebraic (or polynomial) relations $\underset{\sim}{R}$. If $G = G_Q$ is a linear algebraic group over Q with relations $\underset{\sim}{R}$, then $G_{\hat{Q}_{(p)}}$, $G_{\hat{Z}_{(p)}}$ and $G_{\hat{U}_{(p)}}$ are the corresponding matrix groups with the same relations $\underset{\sim}{R}$ but with matrices of p-adic numbers, p-adic integers and p-adic units (whose inverses are also matrices with p-adic integers). $G_{\hat{Q}_{(\infty)}} = G_{\mathbb{R}}$ is the corresponding matrix group with real matrices.

Definition 13.1. $G_A = \{(T_\infty, T_2, T_3, T_5, \ldots, T_p, \ldots) \mid T_p \in G_{\hat{Q}_{(p)}}$ for all places $p = \infty, 2, 3, \ldots$ and $T_p \in G_{\hat{Z}_{(p)}}$ for almost all $p\}$ is called the *adèle group* of G .

If G is the additive group Q then $G_A = A$, and if G is the multiplicative group Q* then $G_A = I$.

Addition and multiplication in G_A are again defined component-wise. $\rho(T) = (T,T,T,\ldots,T,\ldots)$ with $T \in G$ is a *principal adèle* and G and $\rho(G) \subseteq G_A$ can be identified as before. Again $\rho(G)$ is discrete in G_A and G_A is locally compact (with respect to the product topology).

Definition 13.2. $G_A^\infty = G_{\mathbb{R}} \times G_{\hat{Z}_{(2)}} \times G_{\hat{Z}_{(3)}} \times \ldots \times G_{\hat{Z}_{(p)}} \times \ldots \subseteq G_A$.

1.14 Ono [On-1957] defined the idèle group (and the G-genus of lattices with respect to G) for an arbitrary algebraic group G (over an algebraic number field k) and Kneser [Kn-1961] applied the adèle group of the orthogonal group O_f of a (non-degenerate) quadratic form f over Q^n to obtain and extend results by Siegel [Si-1935] on the number of representations of $a \in Q$ by f over Z in terms of the number of representations of $a \in Q$ by f over $\hat{Z}_{(p)}$ (more generally Kneser considers an algebraic number field k instead of Q and an $\underset{\sim}{g}$-module of rank n over the integers $\underset{\sim}{g}$ of k instead of Z^n) .

Kneser [Kn-1961] and Borel [Bo-1963] show for the proper and ordinary orthogonal group $G = O_f^+$, O_f of a non-degenerate quadratic form f over Q (compare also Takahashi [Tak-1957, theorem 5]):

Theorem 14.1. The double cosets $G_A^\infty \cdot T \cdot G_Q$ $(T \in G_A)$ are in one-to-one correspondence with the proper equivalence classes or with the equivalence classes in the genus of f .

Proof. Let $T = (T_\infty, T_2, T_3, \dots, T_p, \dots) \in G_A$. This means that $T_p \in G_{\hat{Q}_{(p)}}$ for all places $p = \infty, 2, 3, \dots$ and $T_p \in G_{\hat{Z}_{(p)}} = G_{\hat{U}_{(p)}}$ for almost all p . We define an action of T on lattices (applied only to the standard lattice Z^n) in Q^n in the following manner. Put $T_p(\hat{Z}^n_{(p)}) = \hat{L}_{(p)}$ which is a local lattice in $\hat{Q}^n_{(p)}$. Then $\hat{L}_{(p)} = \hat{Z}^n_{(p)}$ for almost all p , hence $L = \bigcap_p \hat{L}_{(p)} \cap Q^n$ is a uniquely determined lattice in Q^n (proposition 11.4). We now put $L = TZ^n$. By the definition 11.5 L lies in the same genus as Z^n . The stabilizer of Z^n in G_A is:

$$\begin{aligned}\mathrm{stab}_{G_A} Z^n &= \{T \in G_A \mid TZ^n = Z^n\} \\ &= \{(T_\infty, T_2, T_3, \dots, T_p, \dots) \mid T_p \hat{Z}^n_{(p)} = \hat{Z}^n_{(p)} \quad \text{for all} \quad p\} \\ &= \{(T_\infty, T_2, T_3, \dots, T_p, \dots) \mid T_p \in G_{\hat{Z}_{(p)}} \quad \text{for all} \quad p\} = G_A^\infty \quad .\end{aligned}$$

Hence the cosets $G_A^\infty \cdot T$ with $T \in G_A$ are in one-to-one correspondence with the lattices L in the genus of Z^n , and by the definition 11.1 are the double cosets $G_A^\infty \cdot T \cdot G_Q$ in one-to-one correspondence with the proper or ordinary equivalence classes in the genus of Z^n and hence also with the proper or ordinary equivalence classes of the genus of f by virtue of the proposition 11.3 and 11.7.

2. THE GENUS OF A NILPOTENT GROUP

2.1 Various generalizations of the notion of a genus as defined in 1.11.5 have been introduced by various authors. We only mention Ono [On-1957], where the local orthogonal group $O_{f\mathfrak{p}}$ is replaced by the local algebraic group $G_\mathfrak{f}$ of any algebraic group G over a number field k , Takahashi [Tah-1959], where the genus is defined for Γ-lattices, where Γ denotes the group ring $\mathfrak{g}[G]$ of a finite group G over the integers $\mathfrak{g}$ of an algebraic number field k , and Jacobinski [Ja-1968] where the genus is defined for so called R-lattices. These are finitely generated (unital) R-modules which are torsion free as $\mathfrak{g}$-modules, where R is a subring of a semi-simple finite dimensional algebra A over the quotient field k of a Dedekind ring $\mathfrak{g}$ with the property that $kR = A$ and $1 \in R$ and that R is finitely generated as an $\mathfrak{g}$-module (see also [Sw-1970], p. 106). These definitions paved the way for the notion of a genus of a nilpotent group introduced by Mislin and Pickel.

2.2 We recall that a group G is called *nilpotent* if its lower central series $\gamma_1 G = G$, $\gamma_2 G = [G,G] = \text{group}\{[x,y] = x^{-1}y^{-1}xy \mid x,y \in G\}, \dots, \gamma_{i+1}G = [G, \gamma_i G] = \text{group}\{[x,y] = x^{-1}y^{-1}xy \mid x \in G, y \in \gamma_i G\}, \dots$ is finite, i.e. $\gamma_n G = 1$ for some $n \in N$. A nilpotent group G (the operation in G will be multiplication) admits a unique (up to isomorphism) group G_p for every prime number p , called the *p-localization of* G ([Ma-1949] and [Laz-1954]) satisfying the following properties.

(i) Every $x \in G_p$ has a unique n-th root in G_p for all integers n prime to p ,

(ii) there is a homomorphism $e : G \to G_p$ so that for any other homomorphism $f : G \to K$, where K has the property (i) that all its elements admit unique n-th roots in K for n prime to p , there exists a unique homomorphism $h : G_p \to K$ with $f = h \circ e$.

G_0 is the corresponding group having unique n-th roots in G_0 for all integers n . G_0 is called the *rationalization* of G or else the *Malcev-completion* of G [Ma-1949,2]. It is again unique up to isomorphism. If G is torsion free then G_0 is the smallest divisible group containing G . For more details see [Hil-1975] or [H-M-R-1975].

We also introduce the *p-completion* $\hat{G}_{(p)}$ of G for a prime number p [Su-1970]. This is the set of infinite sequences $\{a_i\}$ with elements in G for which $a_i^{-1}a_{i+1} \in G^{p^i} = gp\{x^{p^i} \mid x \in G\}$, where G^{p^i} is the group generated by the p^i-th power of elements in G . Two sequences $\{a_i\}$ and $\{b_i\}$ are identified if $a_i^{-1}b_i \in G^{p^i}$ for all $i > 0$. The multiplication in $\hat{G}_{(p)}$ is defined coordinate-wise. If G is a finitely generated nilpotent group then also $\hat{G}_{(p)}$

is finitely generated nilpotent and if G is torsion free then so is $\hat{G}_{(p)}$ [Pi-1971].

2.3 In connection with the study and classification of H-spaces Mislin defined the genus $G_M(N)$ of a nilpotent group N as follows ([Mis-1971] and [Mis-1974]).

Definition 3.1. The *Mislin-genus* $G_M(N)$ of the finitely generated nilpotent group N is the set of all isomorphism classes of finitely generated nilpotent groups K with K_p isomorphic to N_p (in symbols $K_p \simeq N_p$) for all primes p.

If $K \in G_M(N)$, we also write $K \underset{M}{\sim} N$.

Pickel was concerned with the isomorphism problem for finitely generated nilpotent groups. He showed that if $\mathcal{F}(G)$ denotes the set of isomorphism classes of finite quotients of the group G and if G and H are finitely generated nilpotent groups, then $\mathcal{F}(G) = \mathcal{F}(H)$ if and only if $\hat{G}_{(p)} \simeq \hat{H}_{(p)}$ for all primes p [Pi-1971, lemma 1.2][1]. This result gave rise to the following definition (given independently of Mislin's definition 3.1).

Definition 3.2. The *Pickel-genus* $G_P(N)$ of the finitely generated nilpotent group N is the set of all isomorphism classes of finitely generated nilpotent groups K with $\hat{K}_{(p)} \simeq \hat{N}_{(p)}$ for all primes p and $K_0 \simeq N_0$.

Pickel showed that $G_P(N)$ is finite [Pi-1971, Section 3] a result that holds all the way through, starting with Gauss (see [On-1957], [Tah-1959], [Eic-1952], [Bo-1963], [Sw-1970, p. 123]). The same holds for the complete genus $G_c(N)$ [Pi-1971, theorem 3.6], defined as follows:

Definition 3.3. The *complete genus* $G_c(N)$ of the finitely generated nilpotent group N is the set of all isomorphism classes of finitely generated nilpotent groups K with $\hat{K}_{(p)} \simeq \hat{N}_{(p)}$ for all primes p.

We shall write $K \underset{P}{\sim} N$ if $K \in G_P(N)$ and $K \underset{c}{\sim} N$ if $K \in G_c(N)$.

[1] *See also [War-1975, lemma 2] for a shorter proof.*

2.4 One has $G_c(N) \supseteq G_P(N) \supseteq G_M(N)$ [War-1975, lemma 3] and in general $G_P(N)$ contains $G_M(N)$ properly [B-W-1975, Cor. 4.2]. This follows from a theorem of Pickel [Pi-1970] who associates with a form f (homogeneous of degree d and in n variables) over $R = Z, Q, Z_p = \{\frac{a}{b}\ a,b \in Z, p \nmid b\}$ or $\hat{Z}_{(p)}$ = the p-adic integers a nilpotent group $N(f)$ so that two forms f and g are R-equivalent up to a unit in R, i.e. $f(A(x)) = u \cdot g(x)$ with $x = (x_1, \dots, x_n) \in R^n$, $A \in GL(n,R)$ and $u \in R^*$ = the units of R, if and only if $N(f)$ is R-isomorphic to $N(g)$. If one now takes the example of Waterhouse (see [B-W-1975, lemma 2.2]) of the two forms of degree 3 in two variables $f = f(x,y) = 7^3y^2((x + \frac{2}{7}y)^3 - 2y^3)$ and $g = g(x,y) = 7^3y^2((x + \frac{1}{7}y)^3 - 2y^3)$ then f and g are equivalent over Z_p and thus over $\hat{Z}_{(p)}$ for all primes $p \neq 7$. Furthermore f and g are equivalent over Q and also over $\hat{Z}_{(7)}$ but not over Z_7 modulo the units of Z_7. Hence $N(f)$ and $N(g)$ are in the same Pickel-genus but not in the same Mislin-genus.

On the other hand Warfield [War-1975, theorem 2 or theorem 4] and Lemaire ([Lem-1975-1] and [Lem-1975-2]) showed independently that $G_P(N) = G_M(N)$ in the case where N is a finitely generated nilpotent group with finite commutator subgroup.

We remark that the set $[X;Y]$ of homotopy classes of continuous maps $f : X \to Y$ (relative to a base point), where X is a finite complex and Y a finite homotopy associative H-complex, forms a finitely generated nilpotent group with finite commutator subgroup.

2.5 Under the same assumption where N is a finitely generated nilpotent group with finite commutator subgroup Mislin and Hilton ([Mis-1974] and [H-M-1975]) were able to introduce a group structure in the genus set $G_M(N) = G_P(N)$ which finds its counterparts in the composition of quadratic forms introduced by Gauss [Ga-1801, art. 235] and in the multiplication of ideals in quadratic number fields (see 3.2).

To that end we introduce the center ZN of N, the torsion subgroup TZN of ZN and the free center FZN of N given by

$$FZN = \{x \in ZN \mid x = y^n \text{ for some } y \in ZN \text{ with } n = \exp TZN = \text{exponent of } TZN\} = (ZN)^n \ .$$

Then FZN is a free abelian characteristic subgroup of N of rank $h = h(N)$, where h equals the dimension of the rationalization of N_0 over Q , and the quotient group $QN = N/FZN$ is finite. We denote by $t(N)$ the exponent of the abelianization of QN , i.e. $t = t(N)$ is the smallest number such that $x^t = 1$ for all $x \in (QN)_{ab} = (QN)/(QN)'$, where $(QN)'$ is the commutator subgroup of QN . ZN , FZN , QN , $h(N)$ and $t(N)$ are all invariants of the genus $G(N) = G_M(N) = G_p(N)$ (see [Mis-1974]).

There is a surjective map $\delta = \delta(N) : (Z/tZ)/*\{\pm 1\} \to G(N)$ of the multiplicative group of congruence classes modulo t which are prime to t , factored by the classes ±1 modulo t to the genus of N [Mis-1974]. If $\bar{a} \in (Z/tZ)^*/\{\pm 1\}$ has a representative $a \in Z$ and if $\delta\bar{a} = M$, then there is a map ϕ of central extensions of Z^h by QN :

$$\begin{tikzcd}
Z^h \arrow[r, tail, "f"] \arrow[d, "\phi_a"'] & N \arrow[r, two heads] \arrow[d, "\phi"] & QN \arrow[d, tail, two heads, "\phi'"] \\
Z^h \arrow[r, tail, "g"] & M \arrow[r, two heads] & QN
\end{tikzcd}$$

where $|a| = |\det \phi_a| = |\text{coker } \phi_a| = [FZM : \phi(FZN)]$, $f(Z^h) = FZN$; $g(Z^h) = FZM$. Furthermore ϕ is injective and surjective modulo elements of order prime to t .

If on the other hand a map ϕ of central extensions of Z^h by QN is given so that ϕ' is an automorphism of QN and that ϕ is injective and surjective modulo elements of order prime to t and $F(Z^h) = FZN$ then $|\text{coker } \phi_a| = |\det \phi_a| = |a|$ is prime to t and $M \in G(N)$ and $g(Z^h) = FZM$. We then put $\delta\bar{a} = M$ where $\bar{a}$ is the congruence class of the order $|\text{coker } \phi_a|$ of coker ϕ_a modulo t . The (additive) abelian group structure in $G(N)$ is now defined to be the unique group structure that extends the surjective map δ to a surjective homomorphism of additive abelian groups. We see that N plays the rôle of a zero-element in $G(N)$.

This construction yields at the same time an upper bound for the cardinality of the genus $G(N)$ (see [H-M-1974] and [Lem-1975-2] for an improvement) and allows one to determine the group structure of $G(N)$ in some special cases. Hilton and Mislin also give a more intrinsic description of the group $G(N)$ by means of pullbacks and pushouts.

3. THE GENUS IN ALGEBRAIC NUMBER FIELDS

In Chapter 1 we followed the stream leading to the concept of a genus for nilpotent groups. Here we would like to mention some other ramifications of Gauss' original genus bringing us to algebraic number fields.

3.1 It was Dedekind [De-1871] who introduced the concept of an ideal in an algebraic number field thereby replacing the ideal numbers that were created by Kummer in order to restall the fundamental theorem of arithmetics (uniqueness of factorization) in algebraic number fields. Dedeking also has given a translation of Gauss' theory of (binary) quadratic forms into the language of ideals [De-1894, Art. 182, 186, 187] which runs as follows.

We consider the quadratic number field $k = Q(\sqrt{d})$ over Q , where d is the *discriminant* of the field k meaning that $d \equiv 1 \pmod 4$ and square free or $d = 4d'$ with $d' \equiv 2$ or $3 \pmod 4$ and d' square free.
$k = Q(\sqrt{d}) = \{r + s\sqrt{d} \mid r,s \in Q\}$ appears as a vector space of dimension 2 over Q and the integers $\underset{\sim}{\mathfrak{o}} = \{a + b\,\frac{d+\sqrt{d}}{2} \mid a,b \in Z\}$ in k form a free Z-module of rank 2 with the basis $1, \theta = \frac{d+\sqrt{d}}{2} \in \underset{\sim}{\mathfrak{o}}$. Every (non zero) ideal $\underset{\sim}{\mathfrak{a}}$ in k is again a free Z-module of rank 2 and can be described as $\underset{\sim}{\mathfrak{a}} = \{x\alpha_1 + y\alpha_2 \mid x,y \in Z\}$ with respect to a certain pair of elements $\alpha_1, \alpha_2 \in \underset{\sim}{\mathfrak{a}}$. We call α_1, α_2 a basis for $\underset{\sim}{\mathfrak{a}}$ and write $\underset{\sim}{\mathfrak{a}} = [\alpha_1, \alpha_2]$. An ideal $\underset{\sim}{\mathfrak{a}}$ in k is said to be *integral* if $\underset{\sim}{\mathfrak{a}} \subseteq \underset{\sim}{\mathfrak{o}}$, otherwise $\underset{\sim}{\mathfrak{a}}$ is called *fractional*. If $\underset{\sim}{\mathfrak{a}}$ is a fractional ideal then there exists a non-zero integer $\beta \in \underset{\sim}{\mathfrak{o}}$ such that $\beta\underset{\sim}{\mathfrak{a}} \subseteq \underset{\sim}{\mathfrak{o}}$.

We let I_k stand for the multiplicative group of (fractional) ideals $\underset{\sim}{\mathfrak{a}}$ in k and P_k for the subgroup of principal ideals $(\alpha) = \alpha\underset{\sim}{\mathfrak{o}}$ generated by a single element $\alpha \in k$. Then the quotient $C_k = I_k|P_k$ is called the *ideal class group* of k . Two ideals $\mathfrak{a}$ and $\mathfrak{a}'$ belonging to the same class in C_k are called *equivalent*, in symbols $\mathfrak{a} \simeq \mathfrak{a}'$; in other words $\mathfrak{a} \simeq \mathfrak{a}'$ iff there exists $\alpha \in k$ such that $\mathfrak{a} = (\alpha)\mathfrak{a}'$. We say that two ideals $\mathfrak{a}$ and $\mathfrak{a}'$ are *properly equivalent*, in symbols $\mathfrak{a} \equiv \mathfrak{a}'$, if there exists $\alpha = a + b\sqrt{d} \in k$ with positive norm $N(\alpha) = \alpha\bar{\alpha} = a^2 - b^2 d > 0$ (see below) and $\mathfrak{a} = (\alpha)\mathfrak{a}'$. That the group C_k as well as the narrower group of proper equivalence classes C_k^0 are finite follows from the finiteness theorem for (proper) equivalence classes of binary quadratic forms (see 1.2 and below).

3.2 We now take an integral ideal $\mathfrak{a} = [\alpha_1, \alpha_2] \subseteq \mathfrak{g}$ with a certain basis $\alpha_1, \alpha_2 \in \mathfrak{a}$. We denote by $N(\mathfrak{a}) = [\mathfrak{g}:\mathfrak{a}]$ the (finite) index of $\mathfrak{a}$ in $\mathfrak{g}$ also called the *norm* of $\mathfrak{a}$. If $\alpha = r + s\sqrt{d}$ is an element in k then $\bar{\alpha} = r - s\sqrt{d}$ is its *conjugate*. The norm $N(\alpha) = \alpha\bar{\alpha} = r^2 - s^2 d$ and the trace $T(\alpha) = \alpha + \bar{\alpha} = 2r$ of α are rational numbers. We shall need the fact that

$N(\mathfrak{a}) = \left|\frac{\alpha_1\bar{\alpha}_2 - \alpha_2\bar{\alpha}_1}{\sqrt{d}}\right|$ (see [Hec-1923, Satz 76, and p. 115]). After ordering the basis elements α_1, α_2 of $\mathfrak{a}$ so that $\alpha_1\bar{\alpha}_2 - \alpha_2\bar{\alpha}_1 = N(\mathfrak{a})\sqrt{d}$ is positive or positive imaginary we associate with the (ordered) ideal $\mathfrak{a} = [\alpha_1, \alpha_2]$ the binary quadratic form

$$f_{\mathfrak{a}} = \frac{(\alpha_1 x + \alpha_2 y)(\bar{\alpha}_1 x + \bar{\alpha}_2 y)}{N(\mathfrak{a})}$$

$$= \frac{\alpha_1\bar{\alpha}_1}{N(\mathfrak{a})} x^2 + \frac{\alpha_1\bar{\alpha}_2 + \alpha_2\bar{\alpha}_1}{N(\mathfrak{a})} xy + \frac{\alpha_2\bar{\alpha}_2}{N(\mathfrak{a})} y^2$$

$$= ax^2 + bxy + cy^2 .$$

From now on it will be more convenient to replace $2b$ in Gauss' notation by b and to introduce the *discriminant* d of $ax^2 + bxy + cy^2$ as being $d = b^2 - 4ac$ which equals four times the determinant in Gauss' sense. We let henceforth $f = (a,b,c)$ stand for the form $ax^2 + bxy + cy^2$ and we shall call (a,b,c) integral if a,b,c are *integral* and *primitive* if the g.c.d. of a,b and c is one.

The coefficients a,b,c in $f_{\mathfrak{a}}$ are integral rational numbers, for the first factor $(x\alpha_1 + y\alpha_2)$ represents a number $\alpha \in \mathfrak{a}$ for all $x,y \in Z$, running through all the elements of $\mathfrak{a}$ if x and y run independently through all of Z , and the second factor $(x\bar{\alpha}_1 + y\bar{\alpha}_2)$ represents the conjugate $\bar{\alpha}$ of α . Hence the product $(x\alpha_1 + y\alpha_2)(x\bar{\alpha}_1 + y\bar{\alpha}_2)$ represents all norms $N(\alpha) = \alpha\bar{\alpha}$ of elements $\alpha \in \mathfrak{a}$ if x and y vary in Z . $N(\mathfrak{a})$ always divides $N(\alpha)$ for all $\alpha \in \mathfrak{a}$, in fact $|N(\alpha)|/N(\mathfrak{a})$ is the index $[\mathfrak{a}:(\alpha)]$ of (α) in $\mathfrak{a}$. $f_{\mathfrak{a}}(x,y)$ is therefore a rational integer for all $(x,y) \in Z^2$, in particular $a = f_{\mathfrak{a}}(1,0)$ and $c = f_{\mathfrak{a}}(0,1)$ and hence $b = f_{\mathfrak{a}}(1,1) - a - c$ are integers. The discriminant $d(f_{\mathfrak{a}})$ is equal to the discriminant of the field $k = Q(\sqrt{d})$,

$$d(f_{\mathfrak{a}}) = b^2 - 4ac = \frac{(\alpha_1\bar{\alpha}_2 + \alpha_2\bar{\alpha}_1)^2 - 4\alpha_1\bar{\alpha}_1\alpha_2\bar{\alpha}_2}{N(\mathfrak{a})^2} = \frac{(\alpha_1\bar{\alpha}_2 - \alpha_2\bar{\alpha}_1)^2}{N(\mathfrak{a})^2} = d .$$

Furthermore the form $f_{\mathfrak{a}}$ must be primitive, for if p divides $a,b,$ and c then p^2 must divide d which is possible only for $p = 2$ (d being a field discriminant) in which case $d = 4d'$ and $d' \equiv 2,3 \pmod 4$. But then the integral quadratic form $\frac{f_{\mathfrak{a}}}{2} = \left(\frac{a}{2}, \frac{b}{2}, \frac{c}{2}\right) = (a',b',c')$ has discriminant $d' = b'^2 - 4a'c'$ which must be $\equiv 0,1 \pmod 4$ contradicting the nature of d' . The primitivity of $f_{\mathfrak{a}}$ implies that $N(\mathfrak{a})$ is the g.c.d. of $\alpha_1\bar{\alpha}_1 = N(\alpha_1)$, $\alpha_1\bar{\alpha}_2 + \alpha_2\bar{\alpha}_1 = T(\alpha_1\bar{\alpha}_2)$ and $\alpha_2\bar{\alpha}_2 = N(\alpha_2)$.

If $d < 0$ then $f_{\mathfrak{a}}$ is a *positive* quadratic form, i.e. $f_{\mathfrak{a}}(Z^2) \geq 0$, because of

$$a = \frac{\alpha_1\bar{\alpha}_1}{N(\mathfrak{a})} = \frac{N(\alpha_1)}{N(\mathfrak{a})} = \frac{r_1^2 - s_1^2 d}{N(\mathfrak{a})} \geq 0$$

(where $\alpha_1 = r_1 + s_1\sqrt{d}$) . If $d > 0$ then $f_{\mathfrak{a}}$ is a so called *indefinite* quadratic form, i.e. a form taking positive and negative values.

We finally notice that a change of basis of $\mathfrak{a}$ yields a form $f'_{\mathfrak{a}}$ properly equivalent to $f_{\mathfrak{a}}$ (see also [Hib-1897, §30]).

Our construction can be summarized by the first part of the following:

Proposition 2.1. To every (ordered integral) ideal $\mathfrak{a} = [\alpha_1,\alpha_2]$ in the field $k = Q(\sqrt{d})$ with discriminant d there corresponds a primitive integral binary quadratic form $f_{\mathfrak{a}}$ of discriminant d which is positive if $d < 0$ and indefinite if $d > 0$.

Conversely, given d there corresponds to every primitive integral binary quadratic form $f = (a,b,c)$ of discriminant $d = b^2 - 4ac$, positive if $d < 0$ and indefinite if $d > 0$, an integral ideal $\mathfrak{a} = [\alpha_1,\alpha_2]$ in the field $Q(\sqrt{d})$ so that $f = f_{\mathfrak{a}}$ (for a proper choice of α_1,α_2).

For the proof of the second part one puts $\mathfrak{a} = \left[a, \frac{b-\sqrt{d}}{2}\right]$ if $d < 0$, or if $d > 0$ and $a > 0$. In the case $d > 0$ and $a > 0$ one puts $\mathfrak{a} = \sqrt{d}\left[a, \frac{b-\sqrt{d}}{2}\right]$. In both cases $\sqrt{d}$ is taken positive or positive imaginary (see [Hec-1923, p. 213]). We have now the following important relation (see [Hec-1923, Satz 154] or [De-1894, §187]).

Proposition 2.2. $\mathfrak{a} \equiv \mathfrak{a}' \Leftrightarrow f_{\mathfrak{a}} \equiv f_{\mathfrak{a}'}$.

Hence there is a one-to-one correspondence between the multiplicative group C_k^0 of proper ideal classes in $k = Q(\sqrt{d})$ and the set of proper primitive equivalence classes of positive quadratic forms (if $d < 0$) or indefinite quadratic forms (if $d > 0$) of discriminant d. This yields on the one hand that the proper ideal class group C_k^0 (as well as the ordinary class group C_k) is finite (see 1.2) and on the other hand that the set of proper primitive equivalence classes of quadratic forms with given discriminant d (positive if $d < 0$, indefinite if $d > 0$) can be equipped with a group structure, the group operation being nothing else than Gauss' *composition* of classes [Ga-1801, Art. 249].

The same correspondence permits to distribute the proper ideal classes of k into genera. Take an ideal class $[\mathfrak{a}]$ with a representative $\mathfrak{a}$ that can be taken integral. Associate to $\mathfrak{a}$ the primitive form $f_{\mathfrak{a}}$. We know (see 1.2) that all forms of the proper class $[f_{\mathfrak{a}}]$ represent the same set $f_{\mathfrak{a}}(Z^2)$ of integers and belong to the same characters, i.e. $\left(\frac{m}{p_i}\right)$ has a fixed value for all $m \in f_{\mathfrak{a}}(Z^2)$ prime to p_i, where p_i is an odd prime divisor of the discriminant d (see 1.2). By the correspondence $\mathfrak{a} \mapsto f_{\mathfrak{a}}$ we see that $f_{\mathfrak{a}}(Z^2)$ is also the set of norms of elements $\alpha \in \mathfrak{a}$ divided by the norm of $\mathfrak{a}$, $f_{\mathfrak{a}}(Z^2) = \left\{\frac{N(\alpha)}{N(\mathfrak{a})} \mid \alpha \in \mathfrak{a}\right\}$. Recall that $N(\alpha)/N(\mathfrak{a})$ is always an integer for any $\alpha \in \mathfrak{a}$. By this and theorem 1.2.3 we infer (see also [Hec-1923, Satz 139])

Theorem 2.3. Let $\mathfrak{a}$ be any (integral) ideal in the proper ideal class $[\mathfrak{a}]$ of the quadratic number field $Q(\sqrt{d})$ with discriminant d and p a prime dividing d. Then the norm $N(\alpha)/N(\mathfrak{a}) \in f_{\mathfrak{a}}(Z^2)$ with non-zero $\alpha \in \mathfrak{a}$ and not divisible by p are all either quadratic residues or non residues modulo p.

It is clear that the construction $\mathfrak{a} \mapsto f_{\mathfrak{a}}$ works as well for fractional ideals, the resulting $f_{\mathfrak{a}}$ still being an integral primitive quadratic form. Clearly proposition 2.2 and theorem 2.3 then still hold in this larger context.

3.3 Hilbert [Hib-1897, §64] (see also [Hib-1894, 2 p. 28]) introduced the *norm residue symbol* $\left(\frac{a,d}{p}\right)$ for an arbitrary integer a, a non-square integer d and any prime p, and he defined

Definition 3.1. $\left(\frac{a,d}{p}\right) = +1$, if $a \equiv N(\alpha) \pmod{p^e}$ for an algebraic integer $\alpha \in \mathfrak{g}$ in the quadratic field $Q(\ d)$ for all powers p^e;

$$\left(\frac{a,d}{p}\right) = -1 \text{ , otherwise.}$$

The symbol has among other the following properties [Hib-1897, §64].

Proposition 3.2.

(i) $\left(\frac{a,d}{p}\right) = 1$, if $p \nmid ad$

(ii) $\left(\frac{a,d}{p}\right) = \left(\frac{a}{p}\right)$, if $p \mid d$, $p \nmid a$ and $p \neq 2$

(iii) $\left(\frac{a,d}{2}\right) = (-1)^{\frac{a-1}{2}}$, if $\frac{d}{4} \equiv 3,7 \pmod 8$

$\left(\frac{a,d}{2}\right) = (-1)^{\frac{a^2-1}{8}}$, if $\frac{d}{4} \equiv 2 \pmod 8$

$\left(\frac{a,d}{2}\right) = (-1)^{\frac{a-1}{2}+\frac{a^2-1}{2}}$, if $\frac{d}{4} \equiv 6 \pmod 8$

(iv) $\left(\frac{ab,d}{p}\right) = \left(\frac{a,d}{p}\right)\left(\frac{b,d}{p}\right)$.[1]

Comparing proposition 3.2 (ii) and (iii) with Section 1.2 we see that Hilbert's norm residue symbol coincides with Gauss' characters or else with Dirichlet's characters $\varepsilon_p(f)$ in the case where those are defined. Recall that $\frac{d}{4}$ is Gauss' determinant of f if d is the discriminant of f . For the field $k = Q(\sqrt{d})$ we get t non-trivial characters $\left(\frac{\ ,d}{p}\right)$, where t is the number of prime divisors of the discriminant d of k . Note that in the case $4 \mid d$ we have only one character corresponding to the prime $p = 2$.

We now want to define the genus of an ideal $\underset{\sim}{a}$ in $Q(\sqrt{d})$ so that $\underset{\sim}{a}$ and $\underset{\sim}{a}'$ are in the same genus iff $f_{\underset{\sim}{a}}$ and $f'_{\underset{\sim}{a}}$ lie in the same (Gauss-) genus. Definition 1.2.5 therefore suggests the following

Definition 3.3. Two ideals $\underset{\sim}{a}$ and $\underset{\sim}{a}'$ or two proper ideal classes $[\underset{\sim}{a}]$ and $[\underset{\sim}{a}']$ in the field $Q(\sqrt{d})$ with discriminant d belong to the same *genus*, in symbols $\underset{\sim}{a} \sim \underset{\sim}{a}'$, if $\varepsilon_p(f_{\underset{\sim}{a}}) = \varepsilon_p(f'_{\underset{\sim}{a}})$ for all odd primes p dividing d and for $p = 2$ if $d \not\equiv 1 \pmod 4$.

Note that the condition for $p = \infty$ (if $d < 0$) is also satisfied.

[1] *By virtue of (iv) the symbol* $\left(\frac{a,d}{p}\right)$ *can be extended to rationals* a , *and one has Proposition 3.2 (v) :* $\left(\frac{a,d}{p}\right) = 1$ *iff* $a \equiv N(\alpha)$ *(mod* p^e*) for an* $\alpha \in Q(\sqrt{d})$ *for all prime powers* p^e . *The symbol is in fact symmetric in* a *and* d , *so that it can be defined for any non-zero rational* d , *but we shall not need this property (see* [Ha-1969]).

We may write $\varepsilon_p(f_{\underset{\sim}{a}}) = \left(\frac{\frac{N(\alpha)}{N(\underset{\sim}{a})}, d}{p}\right)$ for all non-zero $\alpha \in \underset{\sim}{a}$ with $\frac{N(\alpha)}{N(\underset{\sim}{a})}$ prime to p (these α exist because of the primitivity of $f_{\underset{\sim}{a}}$) . Then $\varepsilon_p(f_{\underset{\sim}{a}})$ is defined for all prime numbers, viz. $\varepsilon_p(f_{\underset{\sim}{a}}) = 1$ for all primes p not dividing d by virtue of proposition 3.2 (i) . We could therefore give the following symmetric form to the foregoing definition.

Definition 3.4. $\underset{\sim}{a} \sim \underset{\sim}{a}'$ iff $\varepsilon_p(f_{\underset{\sim}{a}}) = \varepsilon_p(f'_{\underset{\sim}{a}})$ for all primes p where

$$\varepsilon_p(f_{\underset{\sim}{a}}) = \left(\frac{\frac{N(\alpha)}{N(\underset{\sim}{a})}, d}{p}\right)$$

for all non-zero $\alpha \in \underset{\sim}{a}$ with $\frac{N(\alpha)}{N(\underset{\sim}{a})}$ prime to p .

There are at most 2^t different genera, where t is the number of different prime divisors (2 included, if $4 \mid d$) of the discriminant d . It is clear that the unit ideal $(1) = \underset{\sim}{o}$ of all integers in $Q(\sqrt{d})$ lies in the proper principal (ideal) class and hence in the principal genus (by proposition 2.2) which is characterized by $\varepsilon_p(\ ) = +1$ for all primes $p \mid d$ and hence for all p .

The important relations between genera and the norm residue symbol are put together in the following

Theorem 3.5. Let $\underset{\sim}{a}$ and $\underset{\sim}{a}'$ be ideals in the field $Q(\sqrt{d})$ with discriminant d . Then

(i) $\left(\frac{N(\alpha)\ ,\ d}{p}\right) = 1$ for all non-zero $\alpha \in Q(\sqrt{d})$.

(ii) $\underset{\sim}{a}$ is in the principal genus iff $\left(\frac{N(\alpha)\ ,\ d}{p}\right) = 1$ for all primes p .

(iii) $\underset{\sim}{a} \sim \underset{\sim}{a}'$ iff $\left(\frac{N(\underset{\sim}{a})\ ,\ d}{p}\right) = \left(\frac{N(\underset{\sim}{a}')\ ,\ d}{p}\right)$ for all primes p .

(iv) $\underset{\sim}{a}$ is in the principal genus iff there exists $\alpha \in Q(\sqrt{d})$ such that $N(\underset{\sim}{a}) = N(\alpha)$.

(v) $\underset{\sim}{a}$ prime to d is in the principal genus iff there exists $\alpha \in Q(\sqrt{d})$ prime to d such that $N(\underset{\sim}{a}) \equiv N(\alpha) \pmod d$ and $N(\alpha) > 0$.

(vi) $\mathfrak{a} \sim \mathfrak{a}'$ iff there exists $\alpha \in Q(\sqrt{d})$ prime to d such that $N(\mathfrak{a}) \equiv N(\alpha)N(\mathfrak{a}') \pmod{d}$ where $\mathfrak{a}$ and $\mathfrak{a}'$ are prime to d .

Proof.

(i) Follows immediately from definition 3.1 first for integers α and then for any $\alpha \neq 0$ [1] .

(ii) Take an integer $\alpha_p \in \mathfrak{a}$ so that $\frac{N(\alpha_p)}{N(\mathfrak{a})}$ is prime to p . Then $\left(\frac{N(\mathfrak{a})\ ,\ d}{p}\right)\left(\frac{\frac{N(\alpha_p)}{N(\mathfrak{a})}\ ,\ d}{p}\right) = \left(\frac{N(\alpha_p)\ ,\ d}{p}\right) = 1$. $\mathfrak{a}$ is in the principal genus iff $\varepsilon_p(f_{\mathfrak{a}}) = \left(\frac{\frac{N(\alpha_p)}{N(\mathfrak{a})}\ ,\ d}{p}\right) = 1$ for all p (and certain α_p) which is equivalent to say that $\left(\frac{N(\mathfrak{a})\ ,\ d}{p}\right) = 1$ for all p .

(iii) Is a consequence of (ii), and (vi) follows from (v) . To prove (iv) and (v) we shall apply *Hilbert's norm theorem* ([Hib-1837, Satz 102] and [Ha-1969, §26.7]) ,

Theorem 3.6. If for a non-zero n and d $\left(\frac{n,d}{p}\right) = 1$ holds for all primes p , then n is the norm $n = N(\alpha)$ for a non-zero $\alpha \in Q(\sqrt{d})$;

and the *reciprocity law* to which Hilbert has given the form ([Hib-1897, Hilfssatz 14] and [Ha-1969, §5.6]),

Theorem 3.7. For any non-zero n and d , not both negative, the product over all primes $\prod_p \left(\frac{n,d}{p}\right) = 1$.

(iv) Now follows from (ii) and theorem 3.6 and from (i), and (v) can be got from theorem 3.7 as follows. If $N(\mathfrak{a}) \equiv N(\alpha) \pmod{d}$ then $N(\mathfrak{a}) \equiv N(\alpha) \pmod{p}$ for all primes p dividing d which means that $N(\mathfrak{a}) \equiv x^2 - dy^2 \equiv x^2 \pmod{p}$

[1] *By means of the multiplicativity of the norm and Hilbert's norm symbol (proposition 3.2 (iv)).*

is solvable for an integer x mod p . It is well known that then $N(a) \equiv x^2 \pmod{p^e}$ is solvable for all powers p^e of p [Se-1973, II-2, Corollary 2] if $p \neq 2$, hence $\left(\frac{N(\mathfrak{a})\ ,\ d}{p}\right) = 1$ for all $p \neq 2$. By theorem 3.7 and proposition 3.2 (i) also $\left(\frac{N(\mathfrak{a})\ ,\ d}{2}\right) = 1$, so that $\left(\frac{N(\mathfrak{a})\ ,\ d}{p}\right) = 1$ for all primes p . The necessity is clear from (iv).

We now state *Gauss' fundamental theorem for genera* of quadratic number fields $k = Q(\sqrt{d})$ with discriminant d , proven by Gauss for quadratic forms [Ga-1801, Art. 247, 261/2, 286/7] , which can be interpreted today as being the main theorem of class field theory for quadratic number fields.

Theorem 3.8.

(i) There are precisely 2^{t-1} different genera, where t is the number of prime divisors of d .

(ii) The square of any proper ideal class lies in the principal genus, and conversely

(iii) every proper ideal class in the principal genus is the square of a proper ideal class.

Proof. (ii) follows immediately from the multiplicativity of the norm and of Hilbert's norm residue symbol: $\left(\frac{N(\mathfrak{a}^2)\ ,\ d}{p}\right) = \left(\frac{N(\mathfrak{a})\ ,\ d}{p}\right)^2 = +1$ for all primes p . That among the possible 2^t genera there exist at most 2^{t-1} follows from the reciprocity law (theorem 3.7). That there really exist 2^{t-1} genera is a deep lying fact that Gauss was able to deduce via (iii) from the representation theory of binary quadratic forms by ternary quadratic forms.

3.4 The generalization of the theory of genera for quadratic algebraic number fields to cyclic algebraic extension fields of prime degree played an important rôle in erecting the edifice of classical class field theory by Hilbert, Takagi and Hasse.

Suppose that k is an algebraic number field and that K is a cyclic algebraic extension of k, in symbols $K\,|\,k$, whose degree is a prime number ℓ. Then the relative discriminant $\underset{\sim}{d}$ of $K\,|\,k$ is given by $\underset{\sim}{d} = \mathfrak{f}^{\ell-1}$, where $\mathfrak{f}$ is called the *conductor* of $K\,|\,k$ and where $\underset{\sim}{d}$ and $\mathfrak{f}$ are integral ideals in k (see [Hib-1897, Satz. 79] or [Wey-1940, Chap. III, 12]).

First we introduce the *ray modulo* $\mathfrak{f}$ in k, $R_{k,\mathfrak{f}}$, [Web-1897] or [Ha-1926, I, §3] as the multiplicative group of principal ideals $(\alpha) = \alpha\mathfrak{g}$ in k generated by an element $\alpha \in k$ satisfying

(i) $\alpha \equiv 1 \mod \mathfrak{f}$, meaning that $\alpha = \frac{\beta}{\gamma}$ where β and $\gamma \in \mathfrak{g}$ are integer numbers in k prime to $\mathfrak{f}$ and congruent modulo $\mathfrak{f}$,

(ii) $\alpha >> 0$, i.e. α is totally positive, which means that all real conjugates of α are positive.

$R_{k,\mathfrak{f}} = \{(\alpha)\,|\,\alpha \in k\,,\ \alpha \equiv 1 \mod \underset{\sim}{\mathfrak{f}}\,,\ \alpha >> 0\}$ is a subgroup of the group of principal ideals $P_{k,\mathfrak{f}}$ in k prime to $\mathfrak{f}$ which is itself a subgroup of the multiplicative group $I_{k,\mathfrak{f}}$ of ideals in k prime to $\mathfrak{f}$. $S_k = I_{k,\mathfrak{f}}\,|\,R_{k,\mathfrak{f}}$, called the *ray class group* of k, is finite [Ha-1967, p. 72]. We denote by $H_{k,\mathfrak{f}}$ the group of ray classes in k containing relative norms from K to k of ideals $\underset{\sim}{A} \in I_{K,\mathfrak{f}}$ lying in K and prime to $\mathfrak{f}$ and by $Q_{k,\mathfrak{f}}$ the group of ray classes in k containing relative norms of principal ideals $(A) = A\underset{\sim}{O} \in P_{K,\mathfrak{f}}$ lying in K and prime to $\mathfrak{f}$. $Q_{k,\mathfrak{f}}$ is contained in $H_{k,\mathfrak{f}}$ and the norm mapping N from K to k induces a surjective (multiplicative) homomorphism $N_* : I_{K,\mathfrak{f}}\,|\,P_{K,\mathfrak{f}} \to H_{k,\mathfrak{f}}\,|\,Q_{k,\mathfrak{f}}$ whose kernel $E_K = \ker N_*$ is called the *principal genus* in K. It consists of ideal classes $[\underset{\sim}{A}]_{\mathfrak{f}}$ in K prime to $\mathfrak{f}$ whose norm lie in $Q_{k,\mathfrak{f}}$, i.e.

$$E_K = \{[\underset{\sim}{A}]_{\mathfrak{f}}\,|\,\underset{\sim}{A} \subseteq K\,,\ N(\underset{\sim}{A}) \equiv (N(A))\ \ (\mathrm{mod}\ \mathfrak{f})\ \text{ for an } A \in K \text{ with } N(A) >> 0\}\,.\ ^{(1)}$$

$I_{K,\mathfrak{f}}\,|\,E_K$ is the *genera group* in K. Its order $g = [I_{K,\mathfrak{f}}:E_K] = [H_{k,\mathfrak{f}}:Q_{k,\mathfrak{f}}]$ is finite.

Let furthermore τ stand for a generator of the cyclic Galois group of prime order ℓ of K over k, and let $\underset{\sim}{A}^{1-\tau}$ symbolize the quotient $\frac{\underset{\sim}{A}}{\underset{\sim}{A}^{\tau}}$ (see [Hib-1897, §54]) called the symbolic $(1-\tau)$-power of $\underset{\sim}{A}$.

Then Takagi proved [Tak-1920, Sätze 16, 17, 19, 20, 22]

Theorem 4.1.

(i) The symbolic $(1-\tau)$-power of any proper ideal class $[\underset{\sim}{A}]_{\mathfrak{f}} \in C_K$ lies in the principal genus E_K.

(ii) Every proper ideal class $[\underset{\sim}{A}]_{\mathfrak{f}} \in E_K$ is the symbolic $(1-\tau)$-power of a proper ideal class prime to $\mathfrak{f}$ in C_K.

(iii) The number g of genera is given by $g = \frac{[I_{k,\mathfrak{f}}:Q_{k,\mathfrak{f}}]}{\ell}$.

Hereby $\underset{\sim}{A}$ and $\underset{\sim}{B}$ are placed in the same *proper ideal class* in K if $\underset{\sim}{A} = \underset{\sim}{B}(A)$ with $N(A) >> 0$. It is clear that theorem 4.1 generalizes Gauss' theorem 3.8 to cyclic extensions, if we remark that in the quadratic case $\tau^2 = 1$, hence $\tau = -1$ and $1 - \tau = 2$.

We also note that $g = [H_{k,\mathfrak{f}}:Q_{k,\mathfrak{f}}] = \frac{[I_{k,\mathfrak{f}}:Q_{k,\mathfrak{f}}]}{[I_{k,\mathfrak{f}}:H_{k,\mathfrak{f}}]}$ implies that $[I_{k,\mathfrak{f}}:H_{k,\mathfrak{f}}] = \ell$, a fact that will be used in the next definition 4.2.

Takagi applied this theorem 4.1 on the way to establish the existence theorem of class field theory, whereby he defined

Definition 4.2. A relative normal field K over k of relative degree n is said to be *class field* to a group of ray classes $H_{k,\mathfrak{f}}$ modulo an integral ideal $\mathfrak{f}$ in k, if

(1) *We see that* E_K *coincides with the principal genus in quadratic number fields, when* $k = Q$, $K = Q(\sqrt{d})$, $\mathfrak{f} = d$ *(see theorem 3.5 (v)).*

(i) $H_{k,\mathfrak{f}}$ is the group of ray classes in k containing relative norms from K to k of ideals $\mathfrak{A} \in I_{K,\mathfrak{f}}$ lying in K and which are prime to $\mathfrak{f}$.

(ii) $[I_{k,\mathfrak{f}}:H_{k,\mathfrak{f}}] = n$.

The main theorems of class field theory for a given number field k then *comprise* (see [Tak-1920] and [Ha-1926])

Theorem 4.3.

(i) To every group of ray classes $H_{k,\mathfrak{f}}$ modulo an integral ideal $\mathfrak{f}$ in k there exists a unique class field K over k .

(ii) K is abelian over k .

(iii) $I_{k,\mathfrak{f}}/H_{k,\mathfrak{f}}$ is isomorphic to the Galois group of K over k .

(iv) Every abelian field K over k is class field to a group of ray classes $H_{k,\mathfrak{f}}$ modulo an integral ideal $\mathfrak{f}$ in k .

Class field theory therefore establishes a one to one correspondence between abelian extensions of k and certain congruence groups in k .

3.5 Going in the opposite direction Hasse gave an elegant treatment of the theory of genera in the quadratic number field $k = Q(\sqrt{d})$ over Q with discriminant d by means of class field theory [Ha-1951].

Let K be the class field over k belonging to the group of principal ideals (α) generated by $\alpha \in k$ whose norms in Q are positive $N(\alpha) > 0$. K is then the so called *absolute* or *Hilbert class field* in the narrower (or proper) sense. This means that K is abelian over k and unramified over k , i.e. its relative discriminant $\mathfrak{d}$ from K to k is one and the conductor $\mathfrak{f}$ is one also. Moreover K is the maximal unramified abelian extension over k . Hasse now defines [Ha-1951]

Definition 5.1. The maximal unramified abelian extension K_G over k which is also abelian over Q is called the *genus field* of k .

K_G is a subfield of K and it turns out that the group of ray classes $H_{k,\mathfrak{f}}$ $(\mathfrak{f} = 1)$ corresponding to it (i.e. to which K_G is class field over k) is the principal genus E_k in the classical sense, say in the sense of theorem 3.5. Theorem 4.3 (iii) infers that $I_{k,\mathfrak{f}} | E_k$ is isomorphic to the Galois group of K_G over k . Furthermore Hasse regains the fundamental theorem 3.8, viz. the number of genera is $g = [I_{k,\mathfrak{f}}:E_k] = 2^{t-1}$ being also the degree $[K_G:k]$ of K_G over k . More explicitely Hasse determines the genus field K_G as being the composition of independent quadratic fields $Q(\sqrt{p_i^*})$ whose discriminants p_i^* are related to the primes p_i dividing d in the following way

Theorem 5.2. $K_G = Q(\sqrt{p_1^*})(\sqrt{p_2^*})\ldots(\sqrt{p_t^*})$, where $d = p_1^* p_2^* \ldots p_t^*$ is the unique decomposition of the discriminant d into so called prime discriminants of the form

$$p^* = (-1)^{\frac{p-1}{2}} \quad \text{for} \quad p \neq 2$$

$$p^* = -4, \pm 8 \quad \text{for} \quad p = 2$$

if $p | d$.

K_G is of degree 2^t over Q and of degree 2^{t-1} over $k = Q(\sqrt{d})$.

3.6 Based on Hasse's quadratic theory of genera Leopoldt [Leo-1953] developed the more general genus theory for *abelian number fields*.

Let k be an abelian number field over Q and K_G its *genus field* as defined in definition 5.1. The *principal genus* E_k is again defined to be the group of ray classes corresponding to K_G as class field over k , and $I_k | E_k$ [1] is called the *genus group* of k . With the help of the description of the

[1] *Recall that* $\mathfrak{f} = 1$.

arithmetic in abelian number fields by means of characters and Gauss sums [Leo-1962] Leopoldt gave an explicite description of K_G and he obtained the following fundamental theorem.

Theorem 6.1.

(i) The principal genus E_k in k is generated by all symbolic $(1-\tau)$-powers of proper (i.e. narrower) ideal classes $[\mathfrak{a}] \in C_k^\circ$ where τ runs through all automorphisms in the Galois group of k over Q.

(ii) $g = [I_k:E_k] = \dfrac{\prod_p e_p}{[k:Q]}$ the product taken over all prime numbers and where e_p is the ramification order of a prime ideal $\mathfrak{p}$ dividing $p\mathfrak{g}$ in k.

To define the ramification order e_p of the prime number p in k we consider the factorization of the prime ideal $(p) = pZ$ in Q into prime ideals $\mathfrak{p}_1,\dots,\mathfrak{p}_s$ in k $p\mathfrak{g} = \mathfrak{p}_1^{e_1}\dots\mathfrak{p}_s^{e_s}$. It is easy to see that in a Galois (i.e. normal) extension $e_1 = \dots = e_s$ (see [Hec-1923, §29], as all the primes $\mathfrak{p}_1,\dots,\mathfrak{p}_s$ must be conjugate. We call this number the *ramification order* of p in k and denote it by e_p.

A *theorem of Dedekind* ([Hib-1897, Satz 31] and [De-1882]) states that $e_p \neq 1$ if and only if p divides the discriminant d of k over Q.

Furthermore se_p is always a divisor of the field degree $[k:Q]$.

If we apply these remarks to quadratic fields $k = Q(\sqrt{d})$, we get $e_p = 2$ for all primes p that divide the discriminant d and $e_p = 1$ for all the other primes. As $n = [k:Q] = 2$, we get in fact from theorem 6.1 $g = 2^{t-1}$, where t is the number of prime divisors of d. Moreover there are only the two automorphisms 1 = identity and $\tau \neq 1$ with $\tau^2 = 1$; hence $\tau = -1$ and $1 - \tau = 2$. By putting everything together we get as a special case of theorem 6.1 Gauss' theorem 3.8.

On the other hand the specialization of theorem 6.1 (i) to cyclic extensions yields Takagi's theorem 4.1 (i) and (ii) and the specialization of theorem 6.1 (ii) to cyclic extensions gives an expression of the genus number already found by Iyanaga and Tamagawa [I-T-1951] in this cyclic case.

Finally Hasse [Ha-1968] gave a description of the principal genus in an abelian number field which is identical with theorem 3.5 (ii), whereby the Hilbert norm residue symbol $\left(\dfrac{\ \ ,d}{p}\right)$ for the quadratic field $Q(\sqrt{d})$ is replaced by Hasse's general norm symbol $\left(\dfrac{\ \ ,k}{p}\right)$ for the abelian field k (see [Ha-1933]).

3.7 That there is a more general genus theorem for normal number fields over Q is indicated by the following theorem of Tschebotaröw. Recall that the inertia group $T_\mathfrak{p}$ of a prime ideal $\mathfrak{p}$ in a normal algebraic extension k over Q is the subgroup of the Galois group $\mathrm{Gal}(k,Q)$ of k over Q consisting of all automorphisms leaving all the congruence classes modulo $\mathfrak{p}$ in k invariant [Hib-1894-1]. If k is abelian then all $T_\mathfrak{p}$ for the prime ideals $\mathfrak{p}$ dividing a given prime number p in Z coincide. We then put $T_\mathfrak{p} = T_p$. Hilbert showed that e_p is the order of T_p and that the subfield $k(p)$ of k which is fixed under T_p is the maximal subfield of k over Q in which p is unramified [Hib-1894-1].

The theorem of Tschebotaröw that can be interpreted as being an arithmetic analogue of the monodromy theorem in complex function fields now states [Tsch-1929]

Theorem 7.1. If k is a normal number field over Q, then the composition of all inertia groups $T_\mathfrak{p}$ is the full automorphism group of k over Q: $\prod_\mathfrak{p} T_\mathfrak{p} = \mathrm{Gal}(k,Q)$ the composition $\prod$ taken over all prime ideals $\mathfrak{p}$ in k, and where the composition $\prod_\mathfrak{p} T_\mathfrak{p}$ is the smallest group containing all the groups $T_\mathfrak{p}$.

If L is the subfield of k whose elements are fixed under the operation of $\prod_\mathfrak{p} T_\mathfrak{p}$ then L is the maximal unramified extension over Q contained in k.

Theorem 7.1 implies that $L = Q$. This yields a theorem of Minkowski [Min-1891].

Theorem 7.2. For any algebraic number field $k \neq Q$ over Q there is at least one prime number p that is ramified in k, i.e. that is divided by a power of a prime ideal $\mathfrak{p}^e$, $e \neq 1$, in k.

The corresponding theorem for complex algebraic function fields is precisely the *Weierstrass monodromy theorem* that brings us back to topology.

Theorem 7.3. For any algebraic function field $k = C(x)$ over the field of complex rational functions there is at least one prime $(x-a)$, $a \in C$ that is ramified in k.

Or in topological language:

Any not one-sheeted Riemann surface over C has at least one ramification point, or else:

A Riemann surface over C having no ramification points is one-sheeted over C.

3.8 One of the main motivations to study the genus group of an abelian number field k was to gain information about the structure of the class group of k as the former is a special quotient of the latter. In order to extend this program to arbitrary number fields k (of finite degree over Q) Fröhlich introduced the following generalization of the genus field [Frö-1959].

Definition 8.1. Let k be an arbitrary number field of finite degree. Then the *genus field* K_G of k is the maximal non-ramified (abelian) extension of k of form $k \cdot L$ where L is an abelian number field over Q.

If K_A is the maximal abelian subfield of K_G (or else the maximal abelian subfield of the proper (i.e. narrower) Hilbert class field K of k) over Q, then K_G is the composition of k and $K_A, K_G = k \cdot K_A$. Again the *principal genus* E_k is defined as before as being the group of ray classes in k corresponding to K_G as class field over k, and I_k/E_k is the *genus group* of k ($\mathfrak{f} = 1$, as K_G is non-ramified over k). The *genus number* g is the order of I_k/E_k or else the degree $[K_G:k]$. E_k is the least ideal group in k containing the group of proper (i.e. totally positive) principal ideals P_k° which can be characterized by rational congruence conditions with the help of the norm map from k to Q. In fact, Fröhlich first establishes this property of E_k by extending the characterization of E_k in the cyclic case (see 3.4 p. 50) and relates thereafter E_k with K_G [Frö-1959, Theorem 3].

He then applies the theory to determine the genus group for a normal non-abelian field k of degree 6 over Q as well as for the splitting field k over Q of the polynomial $x^n - a$. In his second paper of the same volume he studies relations between the genus group of a number field and the genus group of one of its subfields allowing him to compute the genus group also in the two non-normal cases where k is a non-cyclic cubic field and where $k = Q\left(\sqrt[e^n]{a}\right)$ with e an odd prime and $a \neq \pm 1$ and e-power free integer [Frö-1959, II, Theorem 5 and 6]. Explicitely the structures are as follows.

Theorem 8.2.

(i) If k is a normal non-abelian number field of degree 6 (over Q) with discriminant d_k, and if M is its unique quadratic subfield with discriminant d_M, then we denote by e_M the number of prime divisors of d_M and by e_k the number of prime divisors p of d_k which are prime to d_M and for which $\left(\frac{d_M}{p}\right) = 1$. The genus group of k is then the direct product of $e_M - 1$ groups of order 2 and of e_k groups of order 3. In particular $g = 2^{e_M - 1} \cdot 3^{e_k}$.

(ii) If k is a non-cyclic cubic field of discriminant $d_k = df^2$, where d is the discriminant of $Q(\sqrt{d_k})$ and if e denotes the number of prime divisors p of f with $\left(\frac{d}{p}\right) = 1$, then the genus group of k is the direct product of e groups of order 3. In particular $g = 3^e$.

(iii) If k is the splitting field of the polynomial $x^n - a$ over Z, then its genus group is the direct product of cyclic groups of order $(n,p-1)$, where p is running through all prime divisors of a not dividing n. Hence

$$g = \prod_{p \mid \frac{a}{(a,n)}} (n,p-1) .$$

(iv) The genus group of $k = Q\left(\sqrt[e^n]{a}\right)$, where e is an odd prime and $a \neq \pm 1$ an e-power free integer, is the direct product of cyclic groups of order $(e^n,p-1)$, p running through the prime divisors of a. Hence $g = \prod_{p\mid a} (e^n,p-1)$. As g divides the proper (i.e. narrower) class number h of k we get in each case a lower bound for h.

3.9 In order to construct the genus field K_G of a normal number field Butts [Bu-1973] builds on an idea in Speiser's proof [Sp-1919] of *Kronecker's theorem*:

Every abelian extension of Q is contained in a cyclotomic field $Q(\zeta_n)$, ζ_n being a primitive n-th root of unity.

We shall begin with the easier abelian case.

Theorem 9.1. Let k be an abelian number field with the distinct ramified primes $p_1,\dots p_s$ (dividing the discriminant of k) having ramification orders $e_1,\dots,e_s$ (in k over Q). Put $e_i = e_i' p_i^{\alpha_i}$ with e_1' prime to p_i $(i = I,\dots,s)$. Let M_i be the subfield of the cyclotomic field $Q(\zeta_{p_i})$ of the p_i-th roots of unity whose degree over Q is e_i', and N_i be the subfield $Q\left(\zeta_{p_i^{\alpha_i+1}}\right)$ of degree $p_i^{\alpha_i}$ over Q if $p_i \neq 2$; or if $p_i = 2$ then N_i is either $Q\left(\zeta_{p_i^{\alpha_i+1}}\right)$ or the maximal real subfield of $Q\left(\zeta_{p_i^{\alpha_i+2}}\right)$. $L_i = M_iN_i$ is the composition of M_i and N_i. Then the genus field K_G of k is the composition of all the abelian fields L_i, $K_G = \prod_{i=1}^{s} L_i$.

Hence one has Leopoldts formula

$$[K_G:Q] = \prod_{i=1}^{s} e_i \quad \text{and} \quad g = \frac{\prod_{i=1}^{s} e_i}{[k:Q]}$$

Now the normal case.

Let k be a normal number field with the distinct ramified primes $p_1,\dots,p_s$ having ramification orders $e_1,\dots,e_s$ in k, i.e.

$p_i\underset{\sim}{g} = (\mathfrak{p}_{i1},\dots,\mathfrak{p}_{ir})^{e_i}$ is the factorization of p_i in k, or else

$p_i\hat{\underset{\sim}{\sigma}}_{(\mathfrak{p}_{ij})} = (\mathfrak{p}_{ij})^{e_i}$ is the factorization of p_i in any of the completions $\hat{k}_{(\mathfrak{p}_{ij})}$ $(j=1,\dots,r)$ over $\hat{Q}_{(p_i)}$, i.e. e_i is also the ramification order of p_i in $\hat{k}_{(\mathfrak{p}_{ij})}$ for any $j = 1,\dots,r$. As usual $\underset{\sim}{g}$ denotes the integers in k and $\hat{\sigma}_{(\mathfrak{p}_{ij})}$ stands for the integers in $\hat{k}_{(\mathfrak{p}_{ij})}$. Consider the maximal abelian subfield $A_{(p_i)}$ of any of the completions $\hat{k}_{(\mathfrak{p}_{ij})}$ $(j=1,\dots,r)$ over $\hat{Q}_{(p_i)}$ and call the ramification order e_i' of p_i in $A_{(p_i)}$ the *abelian ramification of* p_i *in* k. Put $e_i' = e_i'' p_i^{\alpha_i}$ with e_i'' prime to p_i. As before let M_i be the subfield of $Q\left(\zeta_{p_i}\right)$ of degree e_i'' over Q and N_i be the subfield of $Q\left(\zeta_{p_i^{\alpha_i+1}}\right)$ of degree $p_i^{\alpha_i}$ over Q (or if $p_i = 2$, either $Q\left(\zeta_{p_i^{\alpha_i+1}}\right)$ or the maximal real subfield of $Q\left(\zeta_{p_i^{\alpha_i+2}}\right)$, and $L_i = M_iN_i$.

Theorem 9.2. Then the genus field K_G of k is the composition of k with all the abelian fields L_i, $K_G = k \cdot \prod_{i=1}^{s} L_i = k \cdot L$ where $L = \prod_{i=1}^{s} L_i$.

Hence $[L:Q] = \prod_{i=1}^{s} e_i'$ and

$$g = [K_G:k] = [L:k_0] = \frac{[L:Q]}{[k_0:Q]} = \frac{\prod_{i=1}^{s} e'_i}{[k_0:Q]} \ .$$

where k_0 is the maximal abelian subfield of k over Q .

The equality $[K_G:k] = [L:k_0]$ stems from the fact that $k_0 = L \cap k$ and $K_G = kL$.

The following consequences are noteworthy.

Theorem 9.3.

(i) If $k = Q(\zeta_n)$ is a cyclotomic field (of the n-th roots of unity), then $K_G = k$ and $g = 1$.

(ii) If $k = Q(\sqrt[n]{a}, \zeta_n)$ is a Kummer extension, $n > 2$, $a \neq \pm 1$ square free and odd, and if $p_1, \dots, p_s$ are the prime factors of $\frac{a}{(a,n)}$, then we take for L_i the subfield of $Q\left(\zeta_{p_i}\right)$ over Q of degree $(n,p-1)$. Then $K_G = k \cdot \prod_{i=1}^{s} L_i = k(\theta_1, \dots, \theta_s)$ where θ_i is a primitive element of L_i over Q . Moreover one gets Fröhlich's formula $g = \prod_{p \mid \frac{a}{(a,n)}} (n,p-1)$.

(iii) If $k = Q(\sqrt[n]{a})$ with $(a,n) = 1$, $a \neq \pm 1$ square free and odd, then $K_G = k \cdot \prod_{i=1}^{s} L_i = k(\theta_1, \dots, \theta_s)$, where L_i and θ_i are determined for $Q(\sqrt[n]{a}, \zeta_n)$ according to (ii) . Again $g = \prod_{p \mid \frac{a}{(a,n)}} (n,p-1)$.

Another interesting result obtained by Butts is the following [Bu-1973, p. 59].

Theorem 9.4. Every finite abelian group A is isomorphic to the genus group $I_k/E_k \cong \mathrm{Gal}(K_G,k)$ of infinitely many number fields k .

3.10 A description of the genus field K_G for any algebraic number field was given by Bhaskaran [Bh-1976]. Let p be a prime that factors in k into the distinct prime ideals $\mathfrak{p}_1, \dots, \mathfrak{p}_s$ with ramification orders $e_1, \dots, e_s$, i.e. $p\mathfrak{o} = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_s^{e_s}$. Consider the maximal abelian subfield $A_{(p)}$ over $\hat{Q}_{(p)}$ of the intersection $\bigcap_{i=1}^{s} \hat{k}_{(\mathfrak{p}_i)}$ of all the completions of k with respect to the $\mathfrak{p}_i \mid p$. We denote by e_p^* the ramification order of p in $A_{(p)}$ with respect to $\hat{Q}_{(p)}$ and p^{α_p} shall be the conductor of $A_{(p)}$ over $\hat{Q}_{(p)}$. There exists a unique cyclic field L_p over Q of degree e_p^* and with conductor p^{α_p} .

Theorem 10.1. The genus field K_G of k is the composition of k with all the cyclic fields L_p for which $e_p^* > 1$: $K_G = k \cdot \prod_p L_p$.

Moreover the following relations hold.

Proposition 10.2.

(i) $e_p^* = (e_1, e_2, \dots, e_s, \varphi(p^{\alpha_p}))$ is the greatest common divisor of all the ramification orders of p and of $\varphi(p^{\alpha_p}) = p^{\alpha_p - 1}(p-1)$, except when $e_p^* = 2$ or $p^{\alpha_p} = 8$.

(ii) $e_p^* = ([\hat{U}_{(p)} : N\,\hat{U}_{(\mathfrak{p}_1)}], \dots, [U_{(p)} : N\,\hat{U}_{(\mathfrak{p}_s)}])$; i.e. e_p^* is the greatest common divisor of all the indices of the norm group of the units $\hat{U}_{(\mathfrak{p}_i)}$ of the completion $\hat{k}_{(\mathfrak{p}_i)}$ within the unit group $\hat{U}_{(p)}$ of the p-adic numbers (the norm taken from $\hat{k}_{(\mathfrak{p}_i)}$ to $\hat{Q}_{(p)}$) , except when $p = 2$ and $-1 \in N\,\hat{U}_{(\mathfrak{p}_i)}$ in which case $e_p^* = 2$.

3.11 Furuta extended the notion of the genus field to relative algebraic normal extensions [Fu-1967].

Definition 11.1. Let M be an algebraic number field and k a normal extension of M of finite degree. Then the *genus field* $K_{G,M}$ *of* k *with respect* *to* M is the maximal unramified (abelian) extension of k of form kL where L is an abelian extension of M .

If $K_{A,M}$ is the maximal abelian subfield of $K_{G,M}$ over M then $K_{G,M} = k \cdot K_{A,M}$.

The degree $[K_{G,M}:K] = g_M$ is called the *relative genus number of* k *with respect to* M .

For the relative genus number Furuta discovered the following formula, (see also [Gu-1977]).

Theorem 11.2.

$$g_M = \frac{h_M \prod\limits_{\mathfrak{p}} e'_{\mathfrak{p}}}{[k_0:M][U_M:U'_M]}$$

where h_M is the proper (or narrow) class number of M , $e'_{\mathfrak{p}}$ is the ramification order of the prime ideal $\mathfrak{p}$ of M in the maximal abelian subfield $A_{(\mathfrak{p})}$ of $k_{(\mathfrak{P})}$ over $\hat{M}_{(\mathfrak{p})}$, where $\mathfrak{P} \subseteq k$ and $\mathfrak{P} \mid \mathfrak{p}$, and k_0 is the maximal abelian subfield of k over M . U_M is the group of totally positive units in M , and U'_M is its subgroup of totally positive units being also local norms in all the $\mathfrak{P}$-adic extensions $\hat{k}_{(\mathfrak{P})}$ (with respect to $\hat{M}_{(\mathfrak{p})}$) for all prime ideals $\mathfrak{P}$ in k , i.e. if $u \in U'_M$ then there exists for every prime ideal $\mathfrak{P} \in k$ an element $\alpha_{\mathfrak{P}} \in \hat{k}_{(\mathfrak{P})}$ such that $u = N_{\hat{k}_{(\mathfrak{P})}|\hat{M}_{(\mathfrak{p})}} \alpha_{\mathfrak{P}}$.

Finally Gold succeded in giving a characterization of the principal genus for these relative normal extensions by means of Hasse's general norm residue symbols [Go-1976] so generalizing Hasse's characterization in the case of abelian extensions over the rationals Q .

BIBLIOGRAPHY

[A-W-1945] ARTIN-WHAPLES, Axiomatic characterization of fields by the product formula for valuations, Bull. Amer. Math. Soc. 51, (1945), 469-492.

[B-W-1975] BELFI-WILKERSON, Some examples in the theory of p-completions, preprint.

[Bh-1976] BHASKARAN, M., Theory of Genus Field and Local Norm Index for any Algebraic Number Field, Preprint 1976.

[Bo-1963] BOREL, A., Some finiteness properties of adèle groups over number fields, Inst. Hautes Etudes Sci. Publ. Math. No. 16, (1963), 5-30.

[Bu-1973] BUTTS, T.R., On the Genus Field and its Application to Four Problems in Algebraic Number Fields, Ph.D.-Thesis, Michigan State University 1973.

[Ch-1933] CHEVALLEY, C., Sur la théorie du corps de classes dans les corps finis et les corps locaux, J. Fac. Sci., Tokyo Univ. 2, (1933), 365-474.

[Ch-1936] CHEVALLEY, C., Généralisation de la théorie du corps de classes pour les extensions infinies, J. Math. Pures Appl. IX, Vol. 15 (1936), 359-371.

[Ch-1940] CHEVALLEY, C., La théorie du corps de classes, Ann. Math. 41 (1940), 394-418.

[De-1871] DEDEKIND, R., Über die Komposition der binären quadratischen Formen, Supplement X von Dirichlets Vorlesungen über Zahlentheorie; Nachdruck: Über die Theorie der algebraischen Zahlen, XLVII, Vieweg, Braunschweig 1964.

[De-1882] DEDEKIND, R., Über die Diskriminanten endlicher Körper, Abh. K. Ges. Wiss. Göttingen 29, (1882), 1-56; Gesammelte mathematische Werke Bd 1, XIX, Chelsea 1969.

[De-1894] DEDEKIND, R., Über die Theorie der ganzen algebraischen Zahlen, Supplement XI von Dirichlets Vorlesungen über Zahlentheorie; Nachdruck, Vieweg, Braunschweig, 1964.

[Di-1839] DIRICHLET, G.L., Recherches sur diverses applications de l'analyse infinitésimale à la théorie des nombres, Crelle, J. reine angew. Mathematik 19 (1839), 324-369, 21, (1840), 134-155; Werke Bd 1, XXVIII, Chelsea 1969.

[Eic-1952] EICHLER, M., Quadratische Formen und orthogonale Gruppen, Springer 1952.

[Eis-1847] EISENSTEIN, G.E., Neue Theoreme der höheren Arithmetik, Crelle, J. reine angew. Mathematik 35 (1847), 117-136.

[Eis-1852] EISENSTEIN, G.E., Vergleich solcher ternaeren quadratischen Formen, welche verschiedene Determinanten haben, Berichte Akademie Wiss. Berlin (1852), 350-387.

[Eu-1754] EULER, L., Demonstratio theorematis Fermationi omnem numerum primum formae $4n + 1$ esse summam duorum quadratorum, Novi comment. acad. scient. Petropolitanae 5, (1754/5), 1760, 3-13; Opera Omnia, Ser. 1, Vol. 2, 328-337, Teubner 1915.

[Fe-1640] Letter of P. FERMAT to M. MERSENNE of December 25, 1640, Oeuvres, Tome 2, 212-217, Gauthier-Villars, Paris 1894.

[Frö-1959] FRÖHLICH, A., The Genus Field and Genus Group in Finite Number Fields, Mathematika 6 (1959), 40-46 and 142-146.

[Fu-1967] FURUTA, Y., The Genus Field and Genus Number in Algebraic Number Fields, Nagoya Math. J. 29 (1967), 281-285.

[Fu-1970] FURUTA, Y., Ueber das Geschlecht und die Klassenzahl eines relativgaloisschen Zahlkörpers vom Primzahlpotenzgrad, Nagoya Math. J. 37 (1970), 197-200.

[Ga-1801] GAUSS, C.F., Disquisitiones arithmeticae, Fleischer, Lipsiae 1801, translated by A. Clarke, Yale University, 1965.

[Ga-1831] GAUSS, C.F., Zusätze zu Seeber's Werke über die ternären quadratischen Formen, Göttingische gelehrte Anzeigen 108 (1831), p. 1074; reprinted in Crelle, J. reine angew. Mathematik 20 (1840), 312-320.

[Go-1976] GOLD, R., Genera in Normal Extensions, Pacific Journal 63 (1976), 397-400.

[Gu-1977] GURAK, S.J., Ideal-Theoretic Characterization of the Relative Genus Field, Preprint 1977.

[Ha-1923-1] HASSE, H., Über die Darstellbarkeit von Zahlen durch quadratische Formen im Körper der rationalen Zahlen, Crelle, J. reine angew. Math. 152, (1923), 129-148.

[Ha-1923-2] HASSE, H., Über die Aequivalenz quadratischer Formen im Körper der rationalen Zahlen, Crelle, J. reine angew. Math. 152, (1923), 205-224.

[Ha-1926] HASSE, H., Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper, I, Ia, II, J-ber dt. Math.-Ver. 35, (1926), 1-55; 36 (1927), 233-311; Exg. Bd 6, (1930), 1-204; Reprint Physica-Verlag, Würzburg 1970.

[Ha-1933-1] HASSE, H., Vorlesungen über Klassen körpertheorie, Universität Marburg 1933; Reprint Physica-Verlag, Würzburg 1967.

[Ha-1933-2] HASSE, H., Die Struktur der R. Brauerschen Algebrenklassengruppe über einem algebraischen Zahlkörper, Math. Ann. 107, (1933), 731-760.

[Ha-1949] HASSE, H., Zahlentheorie, Akademie Verlag, Berlin 1969, 3, Aufl.

[Ha-1951] HASSE, H., Zur Geschlechtertheorie in quadratischen Zahlkörpern, Journ. Math. Soc. Japan, 3,1, (1951), 45-51.

[Ha-1968] HASSE, H., A Supplement to Leopoldt's Theory of Genera in Abelian Number Fields, J. Number Theory 1, (1969), 4-7.

[Hec-1923] HECKE, E., Vorlesungen über die Theorie der algebraischen Zahlen, Teubner, Leipzig 1923; Reprint Chelsea 1970.

[Hen-1908] HENSEL, K., Theorie der algebraischen Zahlen, Teubner, Berlin 1908.

[Hen-1913] HENSEL, K., Zahlentheorie, Göschen, Berlin 1913.

[Hib-1894-1] HILBERT, D., Grundzüge einer Theorie des galoisschen Zahlkörpers, Nachr. Ges. Wiss. Göttingen, (1894), 224-236; Gesammelte Abhandlungen Bd. 1, 4, Springer 1970.

[Hib-1894-2] HILBERT, D., Über den Dirichletschen biquadratischen Zahlkörper, Math. Ann. 45, (1894), 309-340; Gesammelte Abhandlungen Bd. 1, 5, Springer 1970.

[Hib-1897] HILBERT, D., Bericht über die Theorie der algebraischen Zahlkörper, J-ber. Dt. Math.-Ver. 4, (1897), 175-546; Gesammelte Abhandlungen Bd. 1, 7, Springer 1970.

[Hil-1975] HILTON, P., Localization in Topology, Amer. Math. Monthly 82, 2, (1975), 113-131.

[H-M-1975] HILTON-MISLIN, On the genus of a nilpotent group with finite commutator subgroup, Preprint.

[H-M-R-1975] HILTON-MISLIN-ROITBERG, Localization of nilpotent groups and spaces, Mathematics Studies 15, North Holland 1975.

[I-T-1951] IYANAGA-TAMAGAWA, Sur la théorie du corps de classes sur le corps de nombres rationnels, J. Math. Soc. 3, (1951), 220-227.

[Ja-1968] JACOBINSKI, H., Genera and Decomposition of Lattices over Orders, Acta Math. 121, (1968), 1-29.

[Kn-1961] KNESER, M., Darstellungsmasse indefiniter quadratischer Formen, Math. Z. 77, (1961), 188-194.

[Lag-1773] LAGRANGE, J.L., Recherches arithmétiques, Nouv. Mém. de l'Acad. roy. des Sciences et Belles-lettres de Berlin (1773), 263- (1775), 323- ; Oeuvres III, 696-795, Gauthier-Villars, Paris 1869.

[Laz-1954] LAZARD, M., Sur les groupes nilpotents et les anneaux de Lie, Ann. Sc. Ec. N. Sup. 71, (1954), 101-190.

[Lem-1975-1] LEMAIRE, C., On Pickel's Genus of Nilpotent Groups, unpublished.

[Lem-1975-2] LEMAIRE, C., A New Bound for the Genus of a Nilpotent Group, to appear in Comment. Math. Helv.

[Leo-1953] LEOPOLDT, H.W., Zur Geschlechtertheorie in abelschen Zahlkörpern, Math. Nachr. 9, (1953), 351-362.

[Leo-1962] LEOPOLDT, H.W., Zur Arithmetik in abelschen Zahlkörpern, Crelle, J. reine angew. Math. 209, (1962), 54-71.

[Ma-1949-1] MALZEV, A.I., On a Class of Homogeneous Spaces, Izv Akad. Nauk. SSSR, Ser. Mat. 13, (1949), 9-32; English translation, Amer. Math. Soc. Transl. (1) 9, (1962), 276-307.

[Ma-1949-2] MALZEV, A.I., Nilpotent Groups without Torsion, Izv. Akad. Nauk SSSR, Ser. Mat. 13 (1949), 201-212.

[Min-1884] MINKOWSKI, H., Grundlagen für eine Theorie der quadratischen Formen mit ganzzahligen Koeffizienten, Gesammelte Abhandlungen, Bd. 1, I, Chelsea 1967.

[Min-1886] MINKOWSKI, H., Über positive quadratische Formen, Crelle, J. reine angew. Math. 99, (1886), 1-9; Gesammelte Abhandlungen, Bd. 1, III, Chelsea 1967.

[Min-1891-1] MINKOWSKI, H., Über die positiven quadratischen Formen und über kettenbruchartige Algorithmen, Crelle, J. reine angew. Math. 108 (1891), 278-297; Gesammelte Abhandlungen Bd. 1, VIII, Chelsea 1967.

[Min-1891-2] MINKOWSKI, H., Théorèmes arithmétiques, Comptes rendus Acad. Sci., Paris, 112, (1891), 209-212; Gesammelte Abhandlungen Bd. 1, IX, Chelsea 1967.

[Mis-1971] MISLIN, G., The Genus of an H-space, Lecture Notes in Mathematics 249, Springer 1971, 75-83.

[Mis-1974] MISLIN, G., Nilpotent groups with finite commutator subgroups, Lecture Notes in Mathematics 418, Springer 1974, 103-120.

[O'M-1963] O'MEARA, O.T., Introduction to Quadratic Forms, Springer 1963.

[On-1957] ONO, T., Sur une propriété arithmétique des groupes algébriques commutatifs, Bull. Soc. Math. France 85, (1957), 307-323.

[Pi-1970] PICKEL, P.F., Ph.D. Thesis, Rice University, 1970.

[Pi-1971] PICKEL, P.F., Finitely generated nilpotent groups with isomorphic finite quotients, Trans. Amer. Math. Soc. 160, (1971), 327-341.

[Po-1882] POINCARÉ, H., Comptes rendus de l'Académie des Sciences à Paris, 94 (1882), 67-69, 124-127.

[Se-1973] SERRE, J.-P., A course in arithmetic, Springer GTM7, 1973.

[Si-1935] SIEGEL, L., Über die analytische Theorie der quadratischen Formen, Ann. Math. 36, (1935), 527-606; 37, (1936), 230-263; 38 (1937), 212-291).

[Sm-1864] SMITH, H.J.S., On the Orders and Genera of Quadratic Forms Containing more than Three Indeterminates, Coll. Math. Papers I, 412-417, Clarendon Press, Oxford 1896.

[Sm-1867-1] SMITH, H.J.S., On the Orders and Genera of Ternary Quadratic Forms, Coll. Math. Papers I, 455-506, Clarendon Press, Oxford 1896.

[Sm-1867-2] SMITH, H.J.S., On the Orders and Genera of Quadratic Forms Containing more then Three Indeterminants, Coll. Math. Papers I, 510-523, Clarendon Press, Oxford 1896.

[Sp-1912] SPEISER, A., Über die Komposition der binären quadratischen Formen in Festschrift Heinrich Weber, p. 375-395, Chelsea 1971.

[Sp-1919] SPEISER, A., Die Zerlegungsgruppe, J. reine angew. Math. 149 (1919), 174-188.

[Su-1970] SULLIVAN, D., Geometric Topology, Part I, Localization, Periodicity and Galois Symmetry, M.I.T., Cambridge, 1970.

[Sw-1970] SWAN, R.G., K-Theory of Finite Groups and Orders, Springer Lecture Notes in Mathematics 149, Springer 1970.

[Tah-1959] TAKAHASHI, S., Arithmetic of Group Representations, Tôhoku Math. J., 11, (1959), 216-246.

[Tak-1920] TAKAGI, T., Über eine Theorie des relativ-Abelschen Zahlkörpers, Journ. Coll. Science, Tokyo 41, Art. 9, 1920.

[Tsch-1929] TSCHEBOTARËW, N., Zur Gruppentheorie des Klassenkörpers, Crelle, J. reine angew. Math. 161, (1929), 179-193.

[v.d.W.-1955] van der WAERDEN, B.L., Algebra I, Springer, 1955.

[War-1975] WARFIELD, R.B., Genus and Cancellation for Groups with Finite Commutator Subgroups, to appear in J. Pure Appl. Algebra.

[Wat-1960] WATSON, G.L., Integral Quadratic Forms, Cambridge, 1960.

[Web-1897] WEBER, H., Über Zahlgruppen in algebraischen Zahlkörpern, Math. Ann. 48, (1897), 433-473; 49, (1898), 83-100; 50 (1899), 1-26; see also Lehrbuch der Algebra III, §98, §106, §161, Chelsea.

[Wei-1961] WEIL, A., Adèles and Algebraic Groups, Lecture Notes, Princton, 1961.

[Wey-1940] WEYL, H., Algebraic Theory of Numbers, Princton, 1940.

[Wi-1937] WITT, E., Theorie der quadratischen Formen in beliebigen Körpern, Crelle, J. reine angew. Math. 176, (1937), 31-44.

Département de mathématiques
Université Laval
Québec, Québec
G1K 7P4

Manuscrit reçu le 19 octobre 1978.

Ann. Sc. Math. Québec, 1979, Vol. III, No 1, pp. 63-80

CÔNES TANGENTS À UN SOUS-ENSEMBLE CONVEXE FERMÉ

Jean-Pierre Aubin

0. INTRODUCTION

Les *cônes tangents* $T_X(x)$ (où $x \in X$) à un sous-ensemble convexe fermé non vide X d'un espace de Hilbert U jouent un rôle crucial pour démontrer l'existence des points critiques $\overline{x}$ d'une correspondance S , pour montrer que $L + S$ est surjective et pour démontrer l'existence de trajectoires invariantes monotones d'équations différentielles multivoques.

Ceci justifie la présentation "intégrée" des principales propriétés de ces cônes tangents et des moyens de les caractériser.

Après avoir défini les cônes tangents et normaux, nous montrons que $T_X(x) \subset T_Y(x)$ si $x \in X \subset Y$, que $T_{\overline{A(X)}}(Ax) = \overline{AT_X(x)}$, que $T_{X \times Y}(x,y) = T_X(x) \times T_Y(y)$, que $T_{Z \cap Y}(x) = T_Z(x) \cap T_Y(x)$ (lorsque $0 \in \mathrm{Int}\,(Z-Y)$) et plus généralement, que $T_{Z \cap L^{-1}(Y)}(x) = T_Z(x) \cap L^{-1}T_Y(Lx)$ (lorsque $0 \in \mathrm{Int}\,(LZ-Y)$) . On montre de même que si $X = \{y \in Y \text{ tels que } \varphi(y) \leq 1\}$, alors $T_X(x) = T_Y(x) \cap \partial\varphi(x)^{-}$ où $\partial\varphi(x)^{-}$ est le cône polaire négatif du sous-différentiel d'une fonction convexe semi-continue inférieurement φ .

Ces formules permettent de caractériser les cônes tangents à de nombreux ensembles; on "calcule" ainsi les cônes tangents à une boule, un cube, un simplexe et un cône.

* *Annexe à l'article "Analyse fonctionnelle non linéaire et applications" paru dans le Vol. 2, No 1 des Annales.*