Three letters to Walter Feit on group representations and quaternions

Jean-Pierre Serre

Collège de France, 3 rue d’Ulm, 75005 Paris, France

Received 26 September 2005

Communicated by Ronald Solomon
Dedicated to the memory of Walter Feit

Abstract

Representations of the quaternion group by $2 \times 2$ matrices with coefficients in the ring of integers of an imaginary quadratic field.

© 2006 Published by Elsevier Inc.

Keywords: Groups; Quaternions; Representations; Feit; Gauss; Hilbert

Introduction

I have often used my friend Walter Feit as a source of examples and counterexamples in group theory. One such case is [S], on “converse theorems” for the semisimplicity of tensor products. A much older one is the following, which dates from 1974:

Let $\rho : G \to GL_n(K)$ be a linear representation of a finite group $G$ over a number field $K$. Let $O_K$ be the ring of integers of $K$.

Question 1. Can one write $\rho$ over $O_K$, i.e. is $\rho$ conjugate to a homomorphism of $G$ into $GL_n(O_K)$?

It is easy to see that the answer is “yes” if one is allowed to replace $K$ by a suitable finite extension. But, if one refuses such an easy way out, what is the answer?
In more intrinsic terms, let us view \( \rho \) as \( G \to \text{GL}(V) \), where \( V \) is an \( n \)-dimensional \( K \)-vector space. There are \( O_K \)-lattices \( L \) of \( V \) which are stable under the action of \( G \), and Question 1 can be reformulated as:

**Question 1’**. Can one choose \( L \) in such a way that it is free over \( O_K \)?

Recall (cf. e.g. [B, §4, n°10]) that any lattice \( L \) has an *invariant* \( c(L) \) which belongs to the ideal class group \( C_K = \text{Pic}(O_K) \) of \( K \); one may describe \( c(L) \) as the class of the invertible \( O_K \)-module \( \wedge^n L \) in \( \text{Pic}(O_K) \). One has \( c(L) = 0 \) if and only if \( L \) is free.

When I wrote to Feit about this, in 1974, I was not expecting that these questions would always have a positive answer, but I did not know any counterexample. That is what I asked Feit, and the answer was not long in coming. Within a few days, he sent me a proof of:

**Theorem.** (Feit, 1974, unpublished, but see [CRW].) If \( G \) is the quaternion group of order 8, \( K \) is the field \( \mathbb{Q}(\sqrt{-35}) \) and \( \rho : G \to \text{GL}_2(K) \) is irreducible, then the answer to Question 1 is NO.

(In that case, the class group \( C_K \) has order 2, and Feit showed that, if \( L \) is any \( G \)-stable lattice, then \( c(L) \) is the unique non trivial element of \( C_K \).)

This was very satisfactory—except that the role of \( \sqrt{-35} \) was rather mysterious. Of course, if \( K \) is a quadratic field, the irreducible representation \( \rho \) cannot exist unless \( K \) splits the quaternion skew field, which means that \( K \) is imaginary, and that the prime 2 is either inert or ramified in \( K \). There are many such fields, for instance those of the form \( \mathbb{Q}(\sqrt{-N}) \) with \( N > 0 \) and \( N \equiv 3 \pmod{8} \). Which ones would give a NO answer? I discussed this with Feit, and I ended up by proving that (in the above case) one gets a NO answer if and only if \( N \) is divisible, with odd exponent, by a prime \( p \) with \( p \equiv \pm 1 \pmod{8} \); in particular, Feit’s example \( N = 5.7 \) is the smallest such \( N \); other examples are \( N = 51, 91, 115 \), etc. The proof I had at the time was computational. It is only recently (1997) that I noticed that the result can be viewed as a special case of the “genus theory” of Gauss [G] and Hilbert [H]. I wrote this in the form of three letters to Feit. He urged me to publish them. This is what I do now, as a small tribute to an old friend.

Here are the letters:

---

Paris, February 26, 1997

Dear Feit,

Let me take up again—after a 22 years interval—our discussion of your example of a representation of \( Q_8 \) (quaternion group) which cannot be got by a free module.

Let \( K = \mathbb{Q}(\sqrt{-N}) \), where \( N \) is a square-free integer, \( N \equiv 3 \pmod{8} \). Let us denote by \( O_N \) the ring of integers of \( K \); the prime 2 is inert (i.e. \( O_N/2.O_N = F_4 \)); let \( O'_N = O_N[1/2] \). The class groups of \( O_N \) and \( O'_N \) are isomorphic. I denote them by \( C_N \).

The field \( K \) splits the quaternions. Hence there is an irreducible representation of \( G = Q_8 \), of degree 2, over \( K \). Let \( V \) be that representation. We are interested in the following property of \( V \):

1. **There is an** \( O_N \)-free lattice of \( V \) **which is stable under** \( G \) (i.e. the corresponding representation of \( G \) can written with matrices with coefficients in \( O_N \), and not merely with coefficients in \( K \)).
The answer is:

**Theorem.** Property (1) is equivalent to each of the following:

1. $N$ can be written as $x^2 + 2y^2$, with $x, y \in \mathbb{Z}$.
2. Every prime divisor $p$ of $N$ is congruent (mod 8) to either 1 or 3.

(The equivalence of (2) and (3) is elementary.)

This theorem shows, for instance, that (1) is not true if $N = 5q$, where $q$ is any prime with $q \equiv 7 \pmod{8}$. Your $N = 5.7$ is thus the first of an infinite list.

The first step is to look at all possible lattices which are stable under $G$. It is simpler to do so over the ring $O_N' = O_N[1/2]$. Indeed, if $L$ is an $O_N'$-lattice of $V$ stable under $G$, every other such lattice is of the form $aL$, where $a$ is an $O_N'$-fractional ideal (irreducibility of the representation in characteristic $\neq 2$). Hence the invariant of $L$ in the class group $CN$ is well defined up to multiplication by a square. We thus get an invariant $c \in C_N/(C_N)^2$. Property (1) is equivalent to $c = 1$. Hence we have to compute $c$.

Since we are computing in the group $C = C_N/(C_N)^2$, we can take advantage of the “theory of genera,” due essentially to Gauss, which gives a very concrete description of $C$. Let me recall how one does this. Let $S$ be the set of primes dividing $N$, so that $N = \prod_{p \in S} p$. Put $s = |S|$. Gauss’s theory tells us that the elementary 2-group $C$ has rank $s - 1$, and also gives explicit characters $\chi_p : C \to \{\pm 1\}$, for each $p \in S$. More precisely, if $g$ is any element of $C$, we can represent $g$ by an integral ideal $a$ which is prime to $p$; moreover the Legendre symbol $(\frac{N_a}{p})$, where $N_a$ is the norm of $a$, is independent of the choice of $a$ in $g$. One then defines

$$\chi_p : C \to \{\pm 1\}$$

by $\chi_p(g) = (\frac{N_a}{p})$.

The characters $\chi_p$ ($p \in S$) have product 1, and they give an isomorphism of $C$ onto the subgroup of $\{\pm 1\}^S$ consisting of families of $\pm 1$ with product 1.

(From the point of view of class field theory, $\chi_p$ corresponds to the unramified quadratic extension of $K_N$ generated by $\sqrt{p^s}$, with $p^s = \pm p$, $p^s \equiv 1 \pmod{4}$, as usual—I am assuming here that $N$ is not a prime, since in that case $C$ is trivial.)

Let us now come back to the invariant $c$ we want to compute. By the above, this amounts to computing $\chi_p(c)$ for every $p \in S$. The result is the following:

**Formula.** $\chi_p(c) = (\frac{-2}{p})$ for every $p \in S$.

Since $(\frac{-2}{p}) = 1$ if and only if $p \equiv 1, 3 \pmod{8}$, this formula shows that $c = 1$ if and only if condition (3) above is fulfilled. Hence the theorem.

(Moreover, when it is not fulfilled, the formula tells us where the obstruction lies.)

Let me now prove the formula. I follow the starting point of your method. Namely, let $D$ be the standard quaternion field. Since $N \equiv 3 \pmod{8}$, the field $K_N$ can be embedded in $D$. In particular, $O_N$ can be put in $D$ (such an embedding amounts to choosing a decomposition of $N$ as a sum of 3 squares—and, again by Gauss’s *Disquisitiones*, we know that this defines an ideal class of $O_N$—I will not need this). Let $R$ be any maximal order of $D$ containing $O_N$. As you explained in your 1974 letter, we can take for $V$ the $K$-vector space $D$, and we can choose for lattice the maximal order $R$. Hence, if $a$ is the invariant in $C_N$ of the $O_N$-module $R$, our $c$ is just the class of $a$ modulo squares. What we have to do is to compute $\chi_p(a)$ for every $p \in S$. 

---

Please cite this article as: J.-P. Serre, Three letters to Walter Feit on group representations and quaternions, J. Algebra (2006), doi:10.1016/j.jalgebra.2006.01.058.
To do so, notice first that we may write the quaternion algebra \( D \) as \((-N, -x)\), for some \( x \in \mathbb{Q}^* \), since it is split by \( K_N \). Moreover, one sees easily that \( x \) has 2-adic valuation equal to 1 (mod 2), and hence can be chosen of the form \( x = 2a \), where \( a \) is a positive odd square-free integer. This means that \( D \) contains an element \( q \) with
\[
q^2 = -2a, \quad qzq^{-1} = \overline{z} \quad \text{for every} \ z \in K_N.
\]

If you put:
\[
R(N, q) = O_N \oplus qO_N,
\]
once you get an order of \( D \). Choose a maximal order \( R \) containing \( R(N, q) \). Since \( R(N, q) \) is \( O_N \)-free, the invariant of \( R \) is given by the formula:
\[
\text{inv}(R) = \left( \frac{R}{R(N, q)} \right)_K
\]
where I denote by \((M)_K\) the ideal attached to a finite \( O_N \)-module (by Jordan–Hölder). In particular, the norm of that ideal is equal to the index \((R : R(N, q))\) of \( R(N, q) \) in the maximal order \( R \). But that index is easy to compute. One way to do it is to look at the corresponding quadratic form \( N(z) \) of the quaternion algebra. On \( R \), that quadratic form has discriminant \( 2^2 \). On \( R(N, q) \), that form is \( f \oplus 2af \), where \( f \) is the norm form of \( O_N \). Since the discriminant of \( f \) is \(-N\), we thus get the discriminant \((2aN)^2 \). Comparing the two results show that the index we are looking at is equal to \( aN \). Now \( N \) is the norm of the principal ideal generated by \( \sqrt{-N} \). We can suppress it. We thus see that the invariant \( \chi_p(c) \) is given by:

\[
(4) \quad \chi_p(c) = \left( \frac{a}{p} \right) \quad \text{for} \ p \in S.
\]

But we have by assumption \((-1, -1) = (-N, -2a)\). The \( p \)-component of \((-1, -1)\) is trivial, and that of \((-N, -2a)\) is equal to \((-2a)/p \). Hence we have \( (a/p) = (-2a)^{p^{1/2}} \), and (4) gives the formula we wanted. (Note that we end up with a result independent of the auxiliary choice of \( a \), which is reassuring . . .)

Well, that is the proof. Clearly, it can be used in other situations (the “\(-2\)” of the formula being replaced by the “signed square root of the discriminant,” if we were working with a different quaternion algebra).

In the “trivial” case, where \( N \) can be written as \( a^2 + 2b^2 \), one may want to write explicitly a free stable module. I think I have such formulae, but I doubt they are worth writing down . . .

Amitiés

J.-P. Serre

Paris, March 1, 1997

Dear Feit,

About the quaternion business: things look simpler if one views them as in Gauss’s *Disquisitiones* (Art.291, for instance). This amounts to the following (or at least this is how I interpret Gauss):

---

Please cite this article as: J.-P. Serre, Three letters to Walter Feit on group representations and quaternions, J. Algebra (2006), doi:10.1016/j.jalgebra.2006.01.058
I keep the hypothesis of my previous letter, i.e. $N$ is square-free, positive, and $N \equiv 3 \pmod{8}$. (Of course Gauss considers the general case!)

Suppose $N$ is written as a sum of 3 squares:

$$N = a^2 + b^2 + c^2.$$ 

It is easy to see that $a, b, c$ are odd. The main point of Gauss construction is to attach to $(a, b, c)$ an element of the class group $C_N$ of $O_N$, or equivalently, an $O_N$-module of rank 1. Here is the construction: define $L$ as the set of $v = (x, y, z) \in \mathbb{Z}^3$ which are orthogonal to $(a, b, c)$. This is a rank 2 lattice. Moreover, if $p = \sqrt{-N}$ in $O_N$, we can make $p$ act on $L$ by $v \mapsto (a, b, c) \times v = (bz - cy, cx - az, ay - bx)$; because $(a, b, c) \equiv 1 \pmod{2}$, this action of $\mathbb{Z} \times \mathbb{Z}$ on $L$ extends to an action of $O_N$. We thus get the $O_N$-module of rank 1 we wanted. In the language of quadratic forms, the binary quadratic form attached to $L$ is the restriction of the form $(x^2 + y^2 + z^2)/2$; it has discriminant $-N$.

Moreover, the quadratic invariants $\chi_p(L)$ (cf. my previous letter) are equal to $\left( \frac{-2}{p} \right)$, for every prime $p \in S$ (i.e. $p | N$). I am sure that this is also in Gauss, but it is hard to pinpoint it. Anyway, it is easy to prove: one knows that $\chi_p(L)$ can be computed as $\left( \frac{L}{p} \right)$, for any value $t$ of the quadratic form attached to $L$ (provided of course that $t$ be prime to $p$). Here we may take the vector $(-b, a, 0)$ which is in $L$; the value of the quadratic form is $(a^2 + b^2)/2 \equiv -c^2/2 \pmod{p}$.

Hence, its Legendre symbol is $\left( \frac{-2}{p} \right)$, provided that $c \not\equiv 0 \pmod{p}$, which we may assume (if not, replace $c$ by $a$ or $b$).

Hence the class of $L$ lies in a well defined “genus” (i.e. a coset of $C_N$ modulo squares). What Gauss does is to show that every class in that genus is obtainable by a suitable solution of $a^2 + b^2 + c^2 = N$. Moreover, he also counts the number of representations of $N$ as a sum of 3 squares is $24h(-N)$, if $N \equiv 3 \pmod{8}$, $N > 3$ (for $N = 3$, the formula would remain true if one made the convention that $h(-3) = 1/3$).

By the way, do you know of any modern (less than a century old) exposition of these nice results of Gauss (found when he was about 20 years old)? I do not. Fortunately, the Collège de France library has a French translation (dated 1807) of the Disquisitiones, made by a mathematics teacher with the nice name “Poullet-Delisle.” And I got two days ago, as a present from Barcelona, a Catalan translation of the same (Catalan is not very different from French—I can usually guess what it means).

Well, let us apply this to the quaternion problem. Call $D$ the standard quaternions, and $R$ the standard (= Hurwitz) maximal order. We embed $O_N$ in $R$ by mapping $\pi = \sqrt{-N}$ to $ai + bj + ck$, where $a^2 + b^2 + c^2 = N$ as above. We want to determine the ideal class of $R$ as an $O_N$-module (using multiplication on the left).

**Claim.** This ideal class is the class of the module $L$ defined above.

Clearly, this implies what we wanted: $R$ is free over $O_N$ if and only if $L$ is the trivial class, and this will not happen if there exists a prime $p$ dividing $N$ with $\left( \frac{2}{p} \right) = -1$.

Proof of the claim. Look at the exact sequence

$$0 \to O_N \oplus L \to R \to \mathbb{Z}/N\mathbb{Z} \to 0,$$
where I have identified\(^1\) \(L\) (in an obvious way) with a subset of \(R\). As for the map \(R \to \mathbb{Z}/N\mathbb{Z}\), it is defined by \(q \mapsto \text{Tr}(q\pi) \mod N\). Note that this map is \(O_N\)-linear, if we identify \(\mathbb{Z}/N\mathbb{Z}\) with \(O_N/\pi O_N\), i.e. if we make \(\pi\) act by 0 on \(\mathbb{Z}/N\mathbb{Z}\).

The claim follows obviously from the exact sequence, since \(\pi O_N\) is a principal ideal. Done!


Amitiés

J.-P. Serre

Paris, March 26, 1997

Dear Feit,

More on the quaternion business. Some preliminaries first:

1. Gauss’s genera à la Hilbert

Almost exactly one century ago—and one century after Gauss—Hilbert gave an account of genus theory in terms of \((a, b)\) symbols. See his Ges. Abh. I, pp. 161–188. Here it is:

I limit myself to the case of an imaginary quadratic field \(K\), whose discriminant I write as \(-d\), with \(d > 0\); one has \(K = \mathbb{Q}(\sqrt{-d})\). Let \(C\) (or \(C_K\)) be its ideal class group. Genus theory describes \(C/C^2\) by giving explicit homomorphisms of that group in \(\pm 1\). The way Hilbert defines these homomorphisms is by \(a \mapsto (Na, -d)_p\), where \(p\) is a chosen prime divisor of \(d\) and \(Na\) denotes the norm of \(a\). It is easy to see that the sign so obtained does not change when \(a\) is replaced by \(xa\), with \(x \in K^\ast\). An alternate way of viewing these signs is to define a map:

\[
e: C/C^2 \to \text{Br}_2(\mathbb{Q})
\]

by \(e(a) = (Na, -d)\), viewed as an element of the Brauer group of \(\mathbb{Q}\). Gauss’s results can then be formulated as:

(i) \(e\) is injective.

(ii) The image of \(e\) is the subgroup of \(\text{Br}_2(\mathbb{Q})\) consisting of the quaternion algebras unramified at \(\infty\) and at all the primes not dividing \(d\). (Hence, if the number of prime divisors of \(d\) is \(s\), \(C/C^2\) has rank \(s - 1\) because of the product formula.)

(The proof of (i) is elementary. The proof of (ii) requires a little more work, but not much.)

There is a similar theory for real quadratic fields; one has to take into account the fact that the norm of an element \(x\) can be either \(> 0\) or \(< 0\). Hence \(e\) takes values in the quotient of \(\text{Br}_2(\mathbb{Q})\) by the subgroup of order 1 or 2 generated by \((-1, \text{disc}.K)\).

\(^1\) With this identification, the cross product \((a, b, c) \times v(v \in L)\) becomes the quaternion product \(\pi \cdot v\). This is why I had to use left multiplication.
2. Ideal classes attached to quaternion algebras

Let $D$ be any quaternion field over $\mathbb{Q}$ (I do not want to limit myself to the standard case $D = (-1, -1)$). Suppose $K$ is an imaginary quadratic field which splits $D$. Choose an embedding $K \to D$, and a maximal order $O_D$ containing $\mathcal{O}_K$ (ring of integers of $K$). Call $c(O_D)$ the ideal class of $O_D$, viewed as an $\mathcal{O}_K$-module. We have $c(O_D) \in C = C_K$.

**Proposition 1.** The image of $c(O_D)$ in $C/C^2$ does not depend on the choice of $O_D$.

**Proof.** If $L, M$ are different $\mathcal{O}_K$-lattices of a $K$-vector space $V$, denote by $a(L, M)$ the (fractional) ideal of $K$ which measures the relative position of $L, M$ (see Bourbaki AC 7, p. 63). Apply this with $V = D, L = O_D$ and $M = O_D'$ (another maximal order containing $\mathcal{O}_K$). We thus get an ideal $a$ of $K$, and Proposition 1 is equivalent to saying that the class of $a$ is a square. But it is easy to check that $L$ and $M$ have the same volume (their $a$ invariant over $\mathbb{Q}$ is 1—this is a general property of maximal orders of semisimple algebras). Hence the ideal $a$ above is such that $N_a = 1$. The fact that its class is a square follows.

There is a kind of converse to Proposition 1:

**Proposition 2.** Every $c' \in C$ which has the same image as $c(O_D)$ in $C/C^2$ is equal to $c(O_D')$ for some maximal order $O_D'$ containing $\mathcal{O}_K$.

This is not hard to prove, but I shall not need it.

Anyway, Proposition 1 gives us an invariant $c(D, K) \in C/C^2$ which is trivial if (and only if, by Proposition 2) there exists an $O_D$ which is $\mathcal{O}_K$-free. By genus theory à la Hilbert, this $c(D, K)$ is transformed in an element $e(D, K)$ of $Br_2(\mathbb{Q})$. What else can we do except computing $e(D, K)$ explicitly in terms of $D$ and $K$? To do so, let me define the “signed discriminant” $d_D$ of $D$ as:

$$d_D = \pm \text{product of the primes } p \text{ where } D \text{ is ramified,}$$

the sign being $+$ (respectively $-$) if $D$ is unramified at infinity (respectively ramified at infinity).

The square of $d_D$ is what is usually called the “discriminant” of $D$. With this notation, we have:

**Proposition 3.** The invariant $e(D, K)$ is given by:

$$e(D, K) = (D) + (d_D, -d) \quad \text{in } Br_2(\mathbb{Q}),$$

where $(D)$ denotes the class of the quaternion algebra $D$ in $Br_2(\mathbb{Q})$.

**Example.** If $D$ is the standard quaternion algebra $(-1, -1)$, we have $d_D = -2$, hence $e(D, K) = (-1, -1) + (-2, -d) = (-2, d)$. This shows that $O_D$ can be chosen to be $\mathcal{O}_K$-free if and only if $d$ is of the form $x^2 + 2y^2$, with $x, y \in \mathbb{Z}$.

To prove Proposition 3, I use the same method as in my letter of February 26, namely I write $(D)$ as $(x, -d)$ for some $x \in \mathbb{Z}$: this is possible since $K$ splits $D$. Then $D$ contains the order

---

2 The absolute value of $d_D$ is the “reduced discriminant” of $D$, cf. Vignéras [V]. However, the sign is important here.
\[ R = O_K \oplus q.O_K, \text{ where } q \text{ is a quaternion with } q^2 = x, \text{ and } qz = \bar{z}q \text{ for every } z \in K. \] Clearly, \( R \) is \( O_K \)-free. On the other hand, if \( O_D \) is any maximal order of \( D \) containing \( R \), one finds that the index of \( R \) in \( O_D \) is:

\[ (O_D : R) = xd/d_D \quad (\text{note that } x \text{ and } d_D \text{ have the same sign}). \]

This gives us the norm of the \( K \)-ideal \( q(O_D, R) \) and this is all we need to compute \( e(D, K) \); we find:

\[ e(D, K) = (xd d_D, -d). \]

But \( (d, -d) = 0 \), \( (x, -d) = (D) \). Hence we get formula \((\ast)\).

### 3. Application to the representations of \( Q_8 \)

Let us go back to the case \( D = (-1, -1) \) and \( G = Q_8 \), the quaternion group of order 8. We take \( K \) as above, with \( K \) splitting \( D \), and we want to know in what case there is a free rank 2 \( O_K \)-module which gives the standard irreducible representation of \( G \) over \( K \). There are two cases (since \( 2 \) cannot split in \( K \)):

(i) \( 2 \) is unramified and inert in \( K \) (i.e. \( d \equiv 3 \mod 8 \)). In that case, there is only one prime ideal of \( K \) dividing 2, which is 2 itself, and is principal. Hence, the ideal class of a stable lattice gives a well-defined element of \( C/C^2 \), which is the one computed above. We recover the fact that a free lattice exists if and only if \((-2, d) = 0\).

(ii) \( 2 \) is ramified in the field \( K \). In that case, let us call \( a \) the prime ideal of \( K \) of norm 2. The invariant of a stable lattice is then well defined, up to multiplication by a square, and multiplication by a power of \( a \). Since \( e(a) = (2, -d) \) in \( \text{Br}_2(Q) \), we see that a free lattice exists if and only if either \((-2, d) = 0 \) or \((-2, d) = (2, -d) \). The symbol \((2, -d)\) is equal to \((2, d)\). Hence we can rewrite the criterion as:

\[ (-2, d) = 0 \quad \text{or} \quad (-1, d) = 0, \]

i.e.

\[ d \text{ is representable by } x^2 + 2y^2 \text{ or by } x^2 + y^2. \]

**Example.** \( d = 8p \), where \( p \equiv -1 \mod 8 \), \( p \) prime: in that case, no free lattice exists.

Well, that is it. I hope I have not made a mistake in the computation of \((a, b)\) symbols. It would be reassuring if one could write explicitly a free lattice when \( d \) is written either as \( x^2 + 2y^2 \) or \( x^2 + y^2 \); in the first case, the lattice should be stable, not only under \( G = \{ \pm 1, \pm i, \pm j, \pm k \} \), but also under \((1 \pm i \pm j \pm k)/2\).

Amitiés

J.-P. Serre

---

PS. Have you thought of more complicated examples? For instance, \( G = A_n \), and \( K \) the corresponding quadratic field. Explicit case: \( n = 10, K = \mathbb{Q}(\sqrt{21}) \), irreducible representation...
of degree 384 (ATLAS, p. 49). One of the difficulties is that the representation is reducible in several characteristics.

PS 2. A good account of “genus theory” can be found in a book by Venkov on Number Theory (English translation of a Russian book).

References