CONSTRUCTION OF HILBERT 2-CLASS FIELDS

FRANZ LEMMERMEYER

Abstract. Let F be a number field with odd class number, and suppose that k/F is a quadratic extension. We will deal with the problem of constructing parts of the Hilbert 2-class field towers of such fields k.

1. Introduction

We will quickly recall the basic notation: a finite extension K/k of number fields is called

- *unramified* (at the finite primes) if $\operatorname{disc}(K/k) = (1)$;
- *abelian* if K/k is normal with abelian Galois groups;
- *a 2-extension* if K/k is normal with $(K : k)$ a power of 2.

The maximal unramified abelian extension k^1 of k is known to be finite and is called the Hilbert class field of k; the maximal 2-extension of k contained in k^1 is called the Hilbert 2-class field of k. By Artin's reciprocity law, we have $\operatorname{Gal}(k^1/k) \simeq \operatorname{Cl}(k)$. If k/F is abelian, then the maximal extension k_{gen} contained in k^1 which is *abelian* over F is called the *genus class field* of k (with respect to F).

2. The Case $F = \mathbb{Q}$

Let k be a quadratic number field with discriminant $d = \operatorname{disc} k$. Then d is called a *prime discriminant* if exactly one prime p ramifies in $k/\mathbb{Q}$, i.e., if d is a prime power, for example $d = \ldots, -8, -7, -4, -3, 5, 8, 13, \ldots$. It is easy to show that every discriminant d of a quadratic number field can be written uniquely (up to order) as a product of prime discriminants, say $d = d_1 \cdot \ldots \cdot d_t$. The following facts are classical: the 2-class group $\operatorname{Cl}_2^+(k)$ of k in the strict sense has rank $t-1$, and we have $k_{gen} = \mathbb{Q}(\sqrt{d_1}, \ldots, \sqrt{d_t})$. In particular, we can read off the structure of C/C^2, where $C = \operatorname{Cl}(k)$, from the factorization of the discriminant.

This leaves us with the question whether there are similar results for the group C/C^4; an answer was provided by Rédei, Reichardt, and Scholz. From class field theory we deduce that C/C^4 is non-trivial if and only if there exists an unramified cyclic quartic extension K/k. It is not hard to show that $K/\mathbb{Q}$ is normal, and that $\operatorname{Gal}(K/\mathbb{Q}) \simeq D_4$, the dihedral group of order 8. This shows that K contains two quadratic subfields k_1, k_2 other than k, with discriminants d_1 and d_2. It is easily seen that $(d_1, d_2) = 1$, and that not both of them can be negative. By studying the ramification groups of the primes $p \mid d$ and using the fact that they are normal subgroups of the decomposition groups, one deduces that primes $p_1 \mid d_1$ split in k_2 and vice versa. This can also be deduced from the fact that $\mathbb{Q}(\sqrt{d_1}, \sqrt{d_2})$ can be embedded into a dihedral extension of degree 8 (cf. [1]). We find:

Theorem 1. *If K/k is a cyclic unramified quartic extension of a quadratic number field k with $d = \operatorname{disc} k$, then $K/\mathbb{Q}$ is normal with $Gal(K/\mathbb{Q}) \simeq D_4$, and there exist*

relatively prime discriminants d_1, d_2 such that $d = d_1 \cdot d_2$; moreover, for all primes $p_j \mid d_j$, $(j = 1, 2)$, we have

$$\left(\frac{d_1}{p_2}\right) = \left(\frac{d_2}{p_1}\right) = 1. \tag{1}$$

Now there are several ways to prove that the conditions on d in Theorem 1 are sufficient for the existence of an unramified quartic cyclic extension K/k; we will choose the direct approach, namely the explicit construction of K. To this end we note that the conditions 1 guarantee the local solvability of

$$X^2 - d_1Y^2 = d_2Z^2; \tag{2}$$

by the theorems of Legendre and Hasse-Minkowski, there exist primitive solutions (x, y, z) in rational integers (where primitive means that x, y, z are relatively prime). It is an easy exercise in Galois theory to show that $K = k\big(\sqrt{d_1}, \sqrt{x + y\sqrt{d_2}}\big)$ is a cyclic quartic extension of k such that $\mathrm{Gal}\,(K/\mathbb{Q}) \simeq D_4$, and that K/k is unramified outside 2∞. By looking carefully at the ramification above 2 it is possible to show that one can pick the signs of x, y, z in such a way that K/k becomes unramified at 2 also, and this proves

Theorem 2. *Let k be a quadratic number field k with discriminant d, and suppose that $d = d_1 \cdot d_2$ is a factorization of d into relatively prime discriminants d_1, d_2 such that 1 is satisfied. Then the diophantine equation 2 has primitive solutions $(x, y, z) \in \mathbb{Z}^3$, and after a suitable choice of the signs of x, y, the field $K = k\big(\sqrt{d_1}, \sqrt{x + y\sqrt{d_2}}\big)$ is a cyclic quartic extension of k which is unramified outside ∞.*

The construction above can be generalized to other 2-groups of small order; for example, in the quaternionic case we have (the notation of the occuring 2-groups is taken from [4]

Theorem 3. *Let L/k be an unramified H_8-extension of a quadratic number field k, and assume that $L/\mathbb{Q}$ is normal. Then*

1. *$Gal\,(L/\mathbb{Q}) \simeq 32.10 = \Gamma_2 b = (D_4 \curlyvee C_4) \times C_2$;*
2. *there exists a "H_8-factorization" $d = disc\,(k/F) = d_1d_2d_3$ into discriminants such that*
   (a) *L is a quadratic extension of $\mathbb{Q}(\sqrt{d_1}, \sqrt{d_2}, \sqrt{d_3})$;*
   (b) *$(d_i, d_j) = 1$ for $i \neq j$, and*
   (c) *$(d_1d_2/\mathfrak{p}_3) = (d_2d_3/\mathfrak{p}_1) = (d_3d_1/\mathfrak{p}_2) = +1$ for all primes $\mathfrak{p}_i \mid d_i$.*
3. *L is a D_4-extension of $\mathbb{Q}(\sqrt{d_i})$ for $i = 1, 2, 3$ and a $(C_2 \times C_4)-$extension of $\mathbb{Q}(\sqrt{d_1d_2})$, $\mathbb{Q}(\sqrt{d_2d_3})$, and $\mathbb{Q}(\sqrt{d_3d_1})$.*

On the other hand, if $k/\mathbb{Q}$ is a quadratic extension and $d = disc\,(k/\mathbb{Q}) = d_1d_2d_3$ is a H_8-factorization, then there exists an $a \in \mathbb{Z}$ such that $(a, 2) = 1$, $a \nmid d_1d_2$, and such that the system of diophantine equations

$$\begin{cases} d_1X_1^2 - d_2X_2^2 &= -ad_3X_3^2 \\ Y_1^2 - d_1Y_2^2 &= aY_3^2 \\ Z_1^2 - d_2Z_2^2 &= -aZ_3^2 \end{cases} \tag{3}$$

has non-trivial solutions in $\mathbb{Z}$. Let $x_j, y_j, z_j \in \mathbb{Z}$ be a set of primitive solutions of 3, let $r \in \mathbb{Q}^\times$, and put

$$\mu = (x_1\sqrt{d_1} + x_2\sqrt{d_2})(y_1 + y_2\sqrt{d_1})(z_1 + z_2\sqrt{d_2})r;$$

then $L = \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2}, \sqrt{d_3}, \sqrt{\mu}\,)$ *is an* H_8-*extension of* k *such that* $Gal(L/\mathbb{Q}) \simeq \Gamma_2 b$. *Moreover, we can choose* μ *in such a way that* L/k *becomes unramified outside* ∞.

3. Totally real F with class number 1 in the strict sense

In this chapter we will generalize the approach given above by replacing $\mathbb{Q}$ by a field F with class number 1. Let $k = F(\sqrt{\mu}\,)$ be a quadratic extension of F; since F is a principal ideal domain, there exists a relative integral basis of the ring of integers $\mathcal{O}_k$, say $\{1, \alpha\}$. Then the *generalized discriminant* $\delta_k = (\alpha - \alpha')^2$ (where α' denotes the conjugate of α over F) is determined up to squares of units in $\mathcal{O}_F$. This generalized discriminant has all the properties we need: in particular, we have $k = F(\sqrt{\delta_k}\,)$ (for a proof, just observe that $\sqrt{\delta_k} = \alpha - \alpha' \in F(\sqrt{\alpha}\,) \setminus F$). Moreover, for any prime ideal $\mathfrak{p}$ in $\mathcal{O}_F$, the Kronecker symbol

$$(\delta_k/\mathfrak{p}) = \begin{cases} +1, & \text{if } \mathfrak{p} \text{ splits in } k; \\ 0, & \text{if } \mathfrak{p} \text{ ramifies in } k; \\ -1, & \text{if } \mathfrak{p} \text{ is inert in } k. \end{cases}$$

is well defined. A generalized discriminant δ is called *prime* if the ideal $\delta\mathcal{O}_F$ is the power of a prime ideal. Unfortunately, in general we cannot factorize a given discriminant into generalized prime discriminants; in fact, a result due to Goldstein [3], Sunley [9] and Davis [2] shows that such factorizations exist if and only if F is totally real and has class number $h^+ = 1$ in the strict sense. A counter example over $F = \mathbb{Q}(i)$ ($i^2 = -1$) is given by the extension $k = F(\sqrt{1+2i}\,)$, which has generalized discriminant $\delta_k = 2i(1+2i)$, which is neither prime nor the product of two discriminants (there is no quadratic extension of F which is unramified outside $(1+2i)$).

Now the theorems given in Sect. 1 still hold if we replace $\mathbb{Q}$ by totally real fields F with class number 1 in the strict sense, discriminants by generalized discriminants, and rational primes by prime ideals in $\mathcal{O}_F$. We will not give any details, however, because the theorems will generalize even to totally real fields F with odd class number in the strict sense.

4. Totally real F with odd class number in the strict sense

If F has odd class number $h > 1$, then there exist quadratic extensions $k = F(\sqrt{\mu}\,)$ such that $\mathcal{O}_k$ does not have a relative integral basis. In order to find a replacement for the generalized discriminant, we therefore have to proceed in a different way. First we notice that $\mathfrak{d} = \mathrm{diff}\,(k/F)$ is an integral ideal in $\mathcal{O}_k$ generated by elements of the form $\alpha - \alpha'$, $\alpha \in \mathcal{O}_k$. But now the elements $(\alpha - \alpha')\sqrt{\mu}$ are seen to lie in $\mathcal{O}_F$, and since $\mathfrak{d} \mid \sqrt{\mu}\mathcal{O}_k$ this implies that the ideal $\mathfrak{b} = \sqrt{\mu}\mathfrak{d}^{-1}$ is generated by elements in F. Taking the relative norm shows that $\mathrm{disc}\,(k/F)\mathfrak{b}^2 = \mu\mathcal{O}_F$. Now we can choose $\delta \in \mathcal{O}_F$ and $\beta \in F^\times$ such that $\mathrm{disc}\,(k/F)^h = (\delta)$ and $\mathfrak{b}^h = (\beta)$, and the ideal equation $(\delta\beta^2) = (\mu)^h$ shows that we can choose δ in such a way that $\delta\mu$ is a square in F (here we use the fact that h is odd). It is easy to see that δ is determined up to squares of units, and the class δE_F^2 is denoted by $\mathrm{sep}\,(k/F)$ and is called the *separant* of the extension k/F. A separant is called prime if it generates an ideal which is a prime ideal power. The results of Goldstein, Sunley and Davis are contained as a special case in

Theorem 4. *Let F be a number field with odd class number. Then the following assertions are equivalent:*

(1) *The separant of every quadratic extension k/F is the product of prime separants;*
(2) *F is totally real and has odd class number in the strict sense.*

In this case, the factorization into prime separants is necessarily unique (up to order).

Moreover, the results of Section 1 generalize to

Theorem 5. *Let F be a totally real number field with odd class number in the strict sense, and let k/F be a quadratic extension; there exists a $G-$extension K/k which is unramified at the finite places and such that K/F is normal if and only if there is a factorization $d = sep(k/F) = d_1d_2d_3$ into relatively prime separants such that the conditions $(*)$ are satisifed:*

G	$(*)$	$Gal(K/F)$
D_4	$(d_1/\mathfrak{p}_2) = (d_2/\mathfrak{p}_1) = 1$	16.6
H_8	$(d_1d_2/\mathfrak{p}_3) = (d_2d_3/\mathfrak{p}_1) = (d_3d_1/\mathfrak{p}_2) = 1$	16.8
16.9	$(d_1/\mathfrak{p}_2) = (d_1/\mathfrak{p}_3) = (d_2/\mathfrak{p}_1) = (d_3/\mathfrak{p}_1) = 1$	32.33
16.10	$(d_1/\mathfrak{p}_2) = (d_2/\mathfrak{p}_1) = (d_1d_2/\mathfrak{p}_3) = (d_3/\mathfrak{p}_1) = (d_3/\mathfrak{p}_2) = 1$	32.36
$(4,4)$	$(d_i/\mathfrak{p}_j) = 1$ *for all* $i \ne j$	32.34

If $(d_i/\mathfrak{p}_j) = 1$ for all $i \ne j$, there also exists an unramified extension L/k such that $Gal(L/k) \simeq 32.18$ and $Gal(L/F) \simeq 64.144$.

Theor. 5 can probably also be proved by extending a result of Fröhlich from $\mathbb{Q}$ to totally real number fields F with odd class number in the strict sense; cf. [5], where the statement of Theor. 5 for $F = \mathbb{Q}$ is erroneous and its proof contains a gap.

Examples. Let k be an imaginary quadratic number field with discriminant d, and suppose that $d = d_1d_2d_3$ is a factorization of d into discriminants; the following table gives unramified $G-$extensions L/k, where $K = \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2}, \sqrt{d_3}\,)$, for all $2-$groups G occuring in Theor. 5:

G	d	d_1	d_2	d_3	L
D_4	-195	-3	13	5	$K(\sqrt{-1+2\sqrt{-3}}\,)$
H_8	-120	-3	5	8	$K\big(\sqrt{(2\sqrt{2}+\sqrt{5}\,)(2+\sqrt{5}\,)}\,\big)$
16.09	-663	13	17	-3	$K(\sqrt{-1+2\sqrt{-3}}, \sqrt{-1+2\sqrt{13}}\,)$
16.10	-580	5	29	-4	$K(\sqrt{-1+12\sqrt{-1}}, \sqrt{7+2\sqrt{5}}\,)$
$C_4 \times C_4$	-2379	-3	13	61	$K(\sqrt{-19+12\sqrt{-3}}, \sqrt{5+4\sqrt{13}}\,)$

The unramified 32.18−extension of $\mathbb{Q}(\sqrt{-2379}\,)$ predicted by Theor. 7 is obtained by adjoining $\sqrt{-1+2\sqrt{-3}}$ to the $(C_4 \times C_4)-$extension L.

5. The separant class group

We have already seen that there exist number fields with odd class number such that its separants do not factorize into prime separants. This suggests the introduction of "ideal separants" to restore unique factorization; in order to do this we will mimic Dedekind's introduction of ideals as certain sets of algebraic integers.

In our example $F = \mathbb{Q}(i)$ given above, observe that the quadratic extensions $F(\sqrt{a+bi}\,)$, where $a+bi \equiv 3+2i \bmod 4$ is squarefree, have $\operatorname{disc}(k/F) = 2i(a+bi)$ (up to sign, because $E_F^2 = \langle -1 \rangle$). We therefore take the set

$$\sigma = \{2i(a+bi), a+bi \equiv 3+2i \bmod 4 \text{ squarefree}\}$$

as one of the ideal separants occuring in the "prime separant factorization" of $2i(1+2i)$, and

$$\tau = \{\ldots 2i(1+2i), (1+2i)(3+2i), (1+2i)(1-2i), \ldots\}$$

as the other. Of course we would like to have $2i(1+2i) = \sigma\tau$.

Before we can confirm this, we have to find a definition of ideal separants such that they contain the "principal" separants $\operatorname{HSep}(F)$ as a subset, and we have to define a multiplication on the set $\operatorname{ISep}(F)$ of ideal separants in such a way that $\operatorname{HSep}(F)$ becomes a subgroup of $\operatorname{ISep}(F)$. Then we can form the separant class group $\operatorname{SCl}(F) = \operatorname{ISep}(F)/\operatorname{HSep}(F)$ and study its properties.

In order to make $\operatorname{HSep}(F)$ into a group, we define the product of two separants $d_1 = \operatorname{sep}(k_1/F)$ and $d_2 = \operatorname{sep}(k_2/F)$ as follows: the extension $K = F(\sqrt{d_1}, \sqrt{d_2}\,) = k_1k_2$ is a bicyclic biquadratic extension of F; thus it contains a third quadratic subfield k_3, and we put $d_1 * d_2 = \operatorname{sep}(k_3/F)$. This makes $\operatorname{HSep}(F)$ into an elementary abelian 2-group of infinite rank.

For the details of the construction of ISep we refer to [7], and we only note the result:

Theorem 6. *Let F be a number field with odd class number h in the usual and class number $2^u h$ in the strict sense, i.e., let $u = rank Cl_2^+(F)$; moreover, let r and s denote the number of real and complex infinite places of F, respectively. Then*

$$SCl(F) \simeq (\mathbb{Z}/2\mathbb{Z})^{s+u} \simeq E_F^+/E_F^2.$$

In particular, the separant class group is trivial if and only if F is totally real and has odd class number in the strict sense. It is not hard to show that this special case is equivalent to Theorem 4.

The biggest problem remaining is the extension of the definition of a separant to the case where F may have even class number. Once this has been done, one can study the splitting of separants in extensions of number fields, and one may even define a *separant class field* as an extension with the property that exactly the separants in the principal class split completely.

References

[1] P. Damey, J.-J. Payan, *Existence et construction des extensions galoisiennes et non-abéliennes de degré* 8 *d'un corps de caractéristique differente de* 2, J. Reine Angew. Math. **244** (1970), 37–54 1

[2] D. N. Davis, *The prime discriminant factorization of discriminants of algebraic number fields*, Ph. D. Diss. Univ. Florida 1978 3

[3] L. J. Goldstein, *On prime discriminants*, Nagoya Math. J. **45** (1971), 119–127 3

[4] M. Hall, J. K. Senior, *The groups of order* 2^n $(n \leq 6)$, Macmillan New York 1964 2

[5] H. Koch, *Über den* 2*-Klassenkörperturm eines quadratischen Zahlkörpers*, J. Reine Angew. Math. **214/215** (1963), 201–206 4

[6] F. Lemmermeyer, *Explizite Konstruktion von Hilbert-Klassenkörpern*, Diss. Univ. Heidelberg 1995

[7] F. Lemmermeyer, *Separants of quadratic extensions of number fields*, preprint 5

[8] F. Lemmermeyer, *On the* 2*-class field tower of imaginary quadratic number fields*, J. Théorie des Nombres Bordeaux 6 (1994), 261–272

[9] J. Sunley, *Remarks concerning generalized prime discriminants*, Proc. Number Theory Conf. Boulder, Colorado (1972), 233–237 3