J. Austral. Math. Soc. (*Series A*) **51** (1991), 171-186

RIGIDITY OF DECOMPOSITION LAWS AND NUMBER FIELDS

NORBERT KLINGEN

(Received 10 August 1989)

Communicated by H. Lausch

Abstract

We speak of rigidity, if partial information about the prime decomposition in an extension of number fields $K|k$ determines the decomposition law completely (and hence the zeta function ζ_K), or even fixes the field K itself. Several concepts of rigidity, depending on the degree of information we start from, are introduced and studied. The strongest concept (absolute rigidity) was only known to hold for the ground field and all quadratic extensions. Here a complete list of all Galois quartic extensions which are absolutely rigid is given. For the weaker concept of rigidity, all rigid situations among the fields of degree up to 8 are determined.

1980 *Mathematics subject classification* (*Amer. Math. Soc.*) (1985 *Revision*): 11 R 32, 11 R 27, 20 B 25.

1. Introduction

Old results of Gaßmann [7], and more recent results of Jehne [10], Perlis [18], Komatsu [14] and others, showed, that in general, number fields may not be fixed by their decomposition law. There were a lot of examples of extensions K, K' having totally the same decomposition law over some fixed ground field k, without being conjugate over k.

We will introduce and study several concepts of *rigidity*. A decomposition law will be called rigid (see Definition (1.3)), if it is already fixed by some small part of it. We will prove several rigidity results, and for fields up to degree 8 we will determine all rigid situations.

https://doi.org/10.1017/S1446788700034182 Published online by Cambridge University Press

(1.1) Definition. Let $K|k$ be a finite extension of number fields, $\wp$ a prime ideal of k and and $\mathscr{P}_i$ $(i = 1, \dots, r)$ its prime factors in K.

(a) If $f_i = f(\mathscr{P}_i|\wp)$ are the residue degrees, then we call $A = (f_1, \dots, f_r)$ the *type of decomposition* of $\wp$ in K, and for every $r \in \mathbb{N}$ and $A = (f_1, \dots, f_r) \in \mathbb{N}^r$ we let $P_A(K|k)$ be the set of all primes $\wp$ of k having A as type of decomposition in K.

(b) The *(full) decomposition law* of $K|k$ is given by all sets $P_A(K|k)$, while the *weak decomposition law* of K over k is given by the *Kronecker-set*

$$D(K|k) := \{\wp|\wp \text{ has a factor of degree 1 in } K\}.$$

Finally the Kronecker set $D(K|k)$ together with the set

$$S(K|k) := \{\wp|\wp \text{ splits completely in } K\}$$

shall be called the *partial decomposition law* of $K|k$.

By results of Bauer [3], it is well known that two Galois extensions $K|k$, $K'|k$ having almost (that is, up to a finite number of exceptions) the same weak decomposition law must coincide. This does not hold anymore if one of the fields is not Galois; in fact, as mentioned above, there are lots of non-conjugate fields with the same weak, and even full, decomposition law.

(1.2) Examples. (i) (Schinzel [22, page 334]) Every cubic cyclic extension $K|k$ has the same weak decomposition law as some (even infinitely many) sextic fields $K'|k$ (with $K' \supset K$).

(ii) (Klingen [12, Satz 2]) Quintic extensions $K|k$ with normal closure $\tilde{K}$ having Galois group A_5 have the same weak decomposition law as some field $K'|k$ of degree 10.

(iii) (Trinks [24]) Extensions of $K|k$ of degree 7 with Galois group $G(\tilde{K}|k) = \mathrm{GL}_3(2)$ have the same full decomposition law as some non-conjugate septic field $K' \subset \tilde{K}$.

(iv) (Schinzel, Gerst [8, page 138]) The radical extensions $\mathbb{Q}(\sqrt[8]{3})$ and $\mathbb{Q}(\sqrt[8]{48})$ have the same full decomposition law, but are not conjugate over $\mathbb{Q}$.

(1.3) Definition. Let $K|k$ be a finite extension of number fields.

(a) We will call the decomposition law of K over k *absolutely rigid* (respectively *rigid*) if it is already determined by the weak (respectively, by the partial) decomposition law, that is, if any number field K' with the same weak (respectively partial) decomposition law as K has already the same full decomposition law. We will call the decomposition law of K *horizontally rigid*, if it is already determined by the weak decomposition law and the degree $(K : k)$.

(b) We will attribute these properties of rigidity to the field K itself, if not only the full decomposition law, but even the field K is uniquely determined (up to conjugacy over k) by these partial decomposition laws.

https://doi.org/10.1017/S1446788700034182 Published online by Cambridge University Press

(c) We call a number field K *arithmetically* fixed if the full decomposition law determines the field (up to conjugacy), that is, if any field K' with the same full decomposition law is already conjugate. (Perlis [18] calls this *arithmetically solitary.*)

We mention some obvious facts.

'Absolutely rigid' implies 'rigid' and 'horizontally rigid', but (as we will see later on) none of the last two concepts implies the other one.

A field K has one of the three rigidity properties, if and only if its decomposition law has it and additionally K is arithmetically fixed.

The first, and until recently only example of an absolutely rigid field over k was the ground field k itself (Cassels and Fröhlich [6, Exc. 6.2]). This result follows from the fact that a finite group cannot be covered by the conjugates of one subgroup, using the following group theoretical criterion (1.4), (i) $\Leftrightarrow$ (ii), based on the Čebotarev density theorem. That fields with almost the same weak decomposition law (*Kronecker-equivalent* fields, Jehne [10]) must have the same weak decomposition law without any exception was proved in [11, Satz 1].

(1.4) THEOREM. *Let K and K' be extensions of some number field k, $N|k$ a Galois extension containing KK'. Denoting the fixed groups of K (respectively K') in the Galois group $G = G(N|k)$ by U (respectively U'), the following are equivalent:*

(i) *K and K' have almost the same weak decomposition law with respect to k;*

(ii) *the groups U and U' have the same set of conjugate elements in G,*

$$U^G := \bigcup_{\sigma\in G} U^\sigma = U'^G;$$

(iii) *the weak decomposition laws of K and K' agree without any exception.*

The above examples of fields with the same weak decomposition law are constructed using this group theoretical criterion: in the alternating group A_4 the Klein-four group V_4 is covered by the conjugates of any of its subgroups U of order 2;

$$V_4 = V_4^{A_4} = U^{A_4}.$$

Hence, realizing A_4 as Galois group, Theorem (1.4) gives rise to cubic extensions $K|k$ having the same weak decomposition law as some (in fact infinitely many) sextic fields. Since the embedding problem

$$1 \to V_4 \to A_4 \to C_3 \to 1$$

https://doi.org/10.1017/S1446788700034182 Published online by Cambridge University Press

is always properly solvable, this applies to *every* cubic Galois extension $K|k$. Moreover, the infinitely many sextic fields belonging to one cubic field provide examples of fields being rigid, but not horizontally rigid.

2. The alternating and symmetric case

We will see, that all field extensions of degree n with a normal closure having Galois group A_n or S_n are examples of rigid number fields with one exception: the case $G = A_5$ provides us with examples of horizontally rigid, but not rigid number fields. More precisely, we have the following theorem (see Klingen [12]).

(2.1) Theorem. *Let $K|k$ be an extension of degree n with normal closure $\tilde{K}$ over k having Galois group $G = G(\tilde{K}|k) = S_n$ or A_n.*

(a) *If $G \neq A_5$, then K is rigid.*

(b) *If $G = A_5$, then K has the same partial decomposition law as some field $K' \subseteq \tilde{K}$ of degree 10 over k; in particular, K is not rigid.*

(c) *In any case, the field K is horizontally rigid, and therefore also arithmetically fixed.*

Proof. In [12] we proved, for fields K as above, that a field K' Kronecker-equivalent to K over k and contained in $\tilde{K}$ is already conjugate to K, unless we have

$$G = A_5, \qquad G(\tilde{K}|K') = U' := \langle (12)(34), (125) \rangle,$$

in which case $U'^{A_5} = U^{A_5}$ holds for the group $G(\tilde{K}|K) = U = \mathrm{Fix}_{A_5}(5) = A_4$.

This result contains assertion (a), since we know (Bauer [3]) the equivalence of

(i) K and K' have *almost* the same partial decomposition law,

(ii) K and K' have the same weak decomposition law and the same normal closure $\tilde{K} = \widetilde{K'}$ and

(iii) K and K' have the same partial decomposition law.

(b) Since A_5 is simple we must have $\tilde{K} = \tilde{K}'$ and therefore K and K' have the same partial decomposition law. But since they have different degrees, their full decomposition laws differ. (It is well known that two fields with the same full decomposition law have the same zeta function (Cassels and Fröhlich [6, Ex. 6], Perlis [18]) and therefore share many number theoretic invariants (see Klingen [11]), for example, the degree.)

To deduce (c) from (a) one uses the following proposition, the first part

https://doi.org/10.1017/S1446788700034182 Published online by Cambridge University Press

of which is easily proved from (1.4) (see Jehne [10, Reduktionssatz]), while the second statement then follows using the above result of Bauer [3].

(2.2) Proposition. *Let $K|k$ and $K'|k$ be extensions of number fields with the same weak decomposition law, and $\widetilde{K}$, $\widetilde{K'}$ their normal closures over k. Then the fields $K' \cap \widetilde{K}$ and $K \cap \widetilde{K'}$ too, have the same weak decomposition law as K and K'. Hence, if both fields K, K' are minimal with respect to their weak decomposition law, they have the same partial decomposition law.*

To prove (2.1)(c) let K be a field as in the theorem and K' any number field of degree n with the same weak decomposition law, not necessarily contained in $\widetilde{K}$. We choose $K_0 \subseteq K'$ minimal with the same weak decomposition law as K' (and K). Since K has no proper subfield $\neq k$ (the permutation groups A_n, S_n are primitive) and k is absolutely rigid, the fields K and K_0 have the same partial decomposition law according to (2.2), and hence are conjugate by (a). (The exceptional case (b) cannot occur, since we have $(K_0 : k) \leq (K' : k) = n$.) From $(K_0 : k) = (K : k) = n = (K' : k)$, we finally see that $K_0 = K'$ and hence K' is conjugate to K over k.

(2.3) Corollary. *Let $f \in k[X]$ be a polynomial of degree n with Galois group A_n or S_n* (which happens for irreducible polynomials with probability 1), *then for any irreducible polynomial $g \in k[X]$ of degree n the following statements are equivalent:*

(i) *$k(\alpha) = k(\beta)$ for some root α of f and β of g;*

(ii) *The sets $P(f)$ and $P(g)$, where*

$$P(f) := \{\wp \mid \wp | f(a) \textit{ for some } a \in Z_k\},$$

coincide up to a finite number of exceptions.

(Here Z_k denotes the ring of integers of k.) The corollary is clear, since for a root α of f we have $D(k(\alpha)|k) \doteq P(f)$, where $\doteq$ means equality with a finite number of exceptions.

3. Extensions of low degree

As we have seen in the preceding section, in general there is no connection between 'rigid' and 'horizontally rigid', but for extensions of prime power degree, rigidity implies horizontal rigidity: this follows from Proposition (2.2), since fields of prime power degree contain no proper subfield with almost the same weak decomposition law (Klingen [11, Satz 9]).

https://doi.org/10.1017/S1446788700034182 Published online by Cambridge University Press

For fields of prime degree, however, one can even prove the following

(3.1) THEOREM. *Let k be a number field and K an extension of prime degree p.*

(a) *$K|k$ has a horizontally rigid decomposition law,*

(b) *if $K|k$ is solvable by radicals, then even the field K itself is horizontally rigid, and hence in particular arithmetically fixed.*

This theorem was proved in slightly different terms in Klingen [11, Satz 13]. Part (b) is another formulation of the theorem of P. Hall on Hall-subgroups in solvable groups. Part (a) was proved by character theoretic means from the theorem of Burnside that a non-solvable permutation group of prime degree is 2-fold transitive.

In general one cannot deduce in (a) that the decomposition law is rigid, nor can one drop in (b) the assumption of solvability. Counterexamples are given by fields of degree 5 with group A_5 (see (2.1)(b)) and by fields K of degree 7 with normal closure $\tilde{K}$ having as Galois group $G(\tilde{K}|k)$ the simple group $G = \mathrm{GL}_3(2)$ of order 168 with its natural permutation representation of degree 7. Since we have $\mathrm{GL}_3(2) \simeq \mathrm{PSL}_2(7)$ the subgroups of G are well known according to Dickson (see Huppert [9, Kap. II, 8.27]): there are two conjugacy classes of subgroups U, U' isomorphic to S_4, one of which is the fixed group of one element with respect to the permutation representation mentioned above. For these groups we have $U^G = U'^G$, so that the corresponding fields K and K' have the same weak decomposition law. According to (3.1)(a) the full decomposition laws of these fields agree. Since they are not conjugate, we see that we cannot drop the assumption of solvability in (3.1)(b).

Combining the results in the alternating (respectively symmetric) case (Theorem (2.1)) with those in the prime degree case (Theorem (3.1)) one is able to decide for all fields of degree up to 8 whether they are rigid or horizontally rigid.

In the theorem below we use the following notation:

C_n is the cyclic group of order n,

V_4 is the Klein-four-group,

$\mathrm{Aff}(1, R) = \{a \cdot x + b | b \in R, a \in R^\times\}$, the affine group of dimension 1 over a ring R (with $x = \mathrm{id}_R$), and

$G \operatorname{wr} H$ is the wreath product of a group G with a permutation group H.

C. E. Praeger [20] computed independently a list similar to the list of the seven cases below, and I thank her for fruitful discussions on this topic.

(3.2) THEOREM. *Let $K|k$ be an extension of number fields of degree $n \leq 8$ with normal closure $\tilde{K}$, Galois group $G(\tilde{K}|k) := G \subseteq S_n$ and the subgroup $U = \mathrm{Fix}_G(n) \subset G$ fixing K.*

https://doi.org/10.1017/S1446788700034182 Published online by Cambridge University Press

(a) *If there is a non-conjugate field* $K' \subseteq \tilde{K}$, *which has the same weak decomposition law as* K, *then only the following seven cases are possible* (U' *denotes the subgroup of* G *fixing* K').

$$\begin{array}{lll}
n = 5 : G = A_5, & (K' : k) = 10, & U = A_4, \ U' = \langle (12)(34), (125) \rangle . \\
n = 6 : G \simeq A_4, & (K' : k) = 3, & U \subset U' \simeq V_4 . \\
n = 7 : {}^{*}G = \mathrm{GL}_3(2), & (K' : k) = 7, & U \simeq U' \simeq S_4 . \\
n = 8 : {}^{*}G = \mathrm{Aff}(1, \mathbb{Z}/8\mathbb{Z}), & (K' : k) = 8, & U = \langle -x, 3x \rangle, \ U' = \langle -x, 3x+2 \rangle, \\
\quad\ {}^{*}G = \mathrm{GL}_2(3), & (K' : k) = 8, & U \simeq U' \simeq S_3, \\
\quad\ G = C_2 \operatorname{wr} C_4, & (K' : k) = 8, & U = C_2^3 \simeq U' \subset C_2^4 \subset C_2^4 \cdot C_4, \\
\quad\ G = C_2 \operatorname{wr} V_4, & (K' : k) = 8, & U = C_2^3 \simeq U' \subset C_2^4 \subset C_2^4 \cdot V_4 .
\end{array}$$

(b) *Only in the* 3 *cases marked by an asterisk the fields* K, K' *have the same full decomposition law, and hence we deduce the following.*

(α) *The field* K *is arithmetically fixed unless* $G = \mathrm{GL}_3(2)$ ($n = 7$) *or* $G = \mathrm{Aff}(1, \mathbb{Z}/8\mathbb{Z})$ *or* $G = \mathrm{GL}_2(3)$ ($n = 8$).

(β) K *has rigid decomposition law if* $G \neq A_5$, $C_2 \operatorname{wr} C_4$, $C_2 \operatorname{wr} V_4$; K *has a horizontally rigid decomposition law if* $G \neq A_4$ ($n = 6$) *and* $G \neq C_2 \operatorname{wr} C_4$, $C_2 \operatorname{wr} V_4$ ($n = 8$).

(γ) *Apart from the* 6 *cases in* (a) *for* $n = 5, 7, 8$ *the field* K *itself is rigid, while* K *is horizontally rigid unless it belongs to one of the* 6 *cases in* (a) *for* $n = 6, 7, 8$.

(δ) *The last two cases* $n = 8$, $G = C_2 \operatorname{wr} C_4$, $C_2 \operatorname{wr} V_4$ *provide us with the first examples of fields* K, K' *with the same partial decomposition law and the same degree, but different full decomposition laws.*

None of the conditions can be dropped.

Proof. (a) Applying Theorem (1.4) for $N = \tilde{K}$ we get the following group theoretical situation:

$G(N|k) =: G$ a transitive permutation group of degree n;

$G(N|K) =: U$ the subgroup fixing one letter;

$G(N|K') =: U' \subseteq G$ not conjugate to U, but satisfying $U^G = U'^G$, that is, every element of U' fixes one letter.

From Theorem (2.1) we know that, apart from the case $n = 5$, $G = A_5$, we have $G \neq A_n$ and $G \neq S_n$. Hence we have $n \geq 4$.

Case $n = 4$. Since G cannot be abelian, the only permutation group left is the dihedral group of order 8, the group of the square. But then U^G contains exactly three elements and $U^G = U'^G$ implies at once that U' too must be the group fixing one letter, hence conjugate to U, contradicting the assumption.

https://doi.org/10.1017/S1446788700034182 Published online by Cambridge University Press

Case $n = 5$. Here we know from Theorem (3.1) that, in addition to the restrictions already mentioned, G is non-solvable. But then only the case $G = A_5$ remains which according to (2.1)(b) is a true exception.

Case $n = 6$. The exceptional case $G = A_4$ (with its transitive permutation representation of degree 6 given by any of its subgroups of order 2) was already mentioned shortly after Theorem (1.4). To prove that there are no further possibilities we check the list of all transitive permutation groups of degree 6 (see for instance McKay [15]). Since the groups A_6 and S_6 are excluded, the biggest group occurring is the group $\mathrm{PGL}_2(5)$ of order 120. Hence one can check these groups using CAYLEY, the computer system for group theoretical computations.

Case $n = 7$. As for $n = 5$, G must be a non-solvable transitive permutation group of degree 7, different from S_7 and A_7. Hence G is the simple group $\mathrm{GL}_3(2)$ of order 168 with its natural representation of degree 7. Again, this is a true exception already discussed after Theorem (3.1).

Case $n = 8$. The four exceptional cases for $n = 8$ are found on the basis of Butler and McKay's list [5] of all transitive permutation groups of degree 8, again using CAYLEY. The groups are (in the notation of [5]):

$$\begin{aligned}
G &= T15 = \langle (14682357), (17)(28)(36)(45), (34)(78)\rangle \text{ of order } 32,\\
U &= \langle (12)(56), (15)(26)(34)\rangle,\\
U' &= \langle (12)(56), (37)(48)(56)\rangle;\\
G &= T23 = \langle (357)(468), (13)(24)(78)\rangle \text{ of order } 48,\\
U &= \langle (136)(245), (14)(23)(56)\rangle,\\
U' &= \langle (136)(245), (16)(25)(78)\rangle;\\
G &= T27 = \langle (14682357), (12)\rangle \text{ of order } 64,\\
U &= \langle (12), (34), (56)\rangle,\\
U' &= \langle (12)(34)(56), (12)(56)(78), (34)(56)(78)\rangle;\\
G &= T31 = \langle (1625)(37)(48), (17)(28)(35)(46), (12)\rangle \text{ of order } 64,\\
U &= \langle (12), (34), (56)\rangle,\\
U' &= \langle (12)(34)(56), (12)(56)(78), (34)(56)(78)\rangle.
\end{aligned}$$

The first of these four cases for $n = 8$, which has order 32, is realized by the Schinzel and Gerst Example (1.2)(iv). This group therefore is the Galois group $G(\mathbb{Q}(\sqrt[8]{3}, \zeta_8)|\mathbb{Q})$, the affine group $\mathrm{Aff}(1, \mathbb{Z}/8\mathbb{Z})$ with the subgroups U and U' as stated in the theorem. Because of the purely group theoretical

https://doi.org/10.1017/S1446788700034182 Published online by Cambridge University Press

criterion (1.4), Example (1.2)(iv) extends to the following general fact: any octic radical extension $\mathbb{Q}(\sqrt[8]{a})$ has the same weak (in fact full; see the group theoretical criterion $(*)$ in the proof of (b) below) decomposition law as $\mathbb{Q}(\sqrt[8]{16a})$.

The group of order 48 is the general linear group $\mathrm{GL}_2(3)$ in its natural permutation representation on $\mathbb{F}_3^2 \setminus \{0\}$. The subgroup fixing one vector (for example (1,0)) obviously is

$$U = \left\langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \right\rangle .$$

$\mathrm{GL}_2(3)$ has eight conjugacy classes, of which the six non-central ones are characterized by trace and determinant: two classes consisting of the non-diagonalizable matrices with inseparable characteristic polynomial and four cases corresponding to the separable quadratic polynomials over $\mathbb{F}_3$. Besides the unit matrix the subgroup U contains two matrices with trace -1 and determinant 1 and three matrices with trace 0 and determinant -1. The same is true for the subgroup

$$U' = \left\langle \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix} \right\rangle ,$$

which does not fix any non-zero vector, and therefore is not conjugate to U.

As for the last two groups in the list above, we remark that the natural representation of the wreath product $C_2 \operatorname{wr} C_4$ as permutation group on eight letters preserving the partition $(12|34|56|78)$ is given as

$$C_2 \operatorname{wr} C_4 = \langle (12), (1357)(2468) \rangle ,$$

which because of $(1357)(2468)(12) = (14682357)$ is exactly the group $T27$ as given above. Representing the wreath product as semidirect product C_2 wr $C_4 = C_2^4 \cdot C_4$, the subgroup U fixing the letter 8 obviously is given as $U = C_2^3 \subset C_2^4$, that is,

$$U = \langle (1, 0, 0, 0), (0, 1, 0, 0), (0, 0, 1, 0) \rangle ,$$

while, up to conjugacy, we have

$$U' = \langle (0, 1, 1, 1), (1, 0, 1, 1), (1, 1, 0, 1) \rangle .$$

The duality between U and U' is obvious.

Vectors $x = (x_1, \ldots, x_4) \in C_2^4$ are conjugate in the group $G = C_2^4 \cdot C_4$ exactly if the corresponding sets $\{i | x_i = 1\} \subset \{1, \ldots, 4\}$ belong to the same orbit under the regular action of C_4. From this one sees that the groups U and U' determine the same set of conjugate elements. These considerations apply equally well in the last case.

(b) In the first two cases the fields K, K' cannot have the same full

https://doi.org/10.1017/S1446788700034182 Published online by Cambridge University Press

decomposition law, since they are either of different degree $(n = 5)$ or have different normal closures $(n = 6)$. That in the third and fourth case the fields do have the same full decomposition law was mentioned earlier, while in the last three cases one easily tests the following group theoretical criterion (σ^G denotes the conjugacy class of $\sigma \in G$),

$$(*) \qquad \bigwedge_{\sigma \in G} \#(\sigma^G \cap U) = \#(\sigma^G \cap U'),$$

which is equivalent to the fact that the fields K, K' have the same full decomposition law (for example, see Cassels and Fröhlich [6, Exc. 6], Klingen [11, Satz 2]). For $G = \mathrm{GL}_2(3)$ and the groups U, U' as given above the numbers in $(*)$ are $0, 1, 2, 3$ as was explained already in the proof of (a), and agree in both cases.

For the wreath products one checks (with the notations already used) that the conjugacy class consisting of all vectors $x \in C_2^4$ with exactly one non-zero entry meets U in only one element, while it meets U' in 3 elements.

This proves assertions (α) and (δ); (γ) follows from (α) and (β).

As for (β) we first notice, that in the case mentioned in (a) for $n = 6$, the field K' is Galois over k, hence K and K' cannot have the same partial decomposition law, so the decomposition law of K is rigid if $G \neq A_5$. Unless $n = 6$, $G \simeq A_4$, the results of (a) show that K is minimal, even of minimal degree, with respect to Kronecker equivalence. Because of (2.2) we deduce from the rigidity just proved that K is horizontally rigid. This also applies in the case $n = 5$, $G = A_5$, since in that case the fields K and K' are of different degree.

4. Absolutely rigid fields

As was already mentioned in the introduction, until recently the only known result concerning absolute rigidity was the fact that no proper extension K of k can have the same weak decomposition law as the groundfield k itself. The situation is even worse, since Jehne showed [10, Theorem 3] that for many number fields K there exist *infinitely* many others with the same weak decomposition law. This is true especially for all Galois extensions K of odd degree or of degree 8 with cyclic or quaternion Galois group.

However, Jehne [10, remark after Theorem 5] also showed that if quadratic extensions were not absolutely rigid, then a finite simple group G had to exist, which could be covered by the conjugates of *two* maximal subgroups U, U', isomorphic under some outer automorphism of G. This seemed highly improbable, and in fact there were several results excluding a lot of finite simple groups (Jehne [10], Klingen [12], [13], Brandl [4]), but only after

https://doi.org/10.1017/S1446788700034182 Published online by Cambridge University Press

the classification of the finite simple groups was complete Saxl [21] was able to exclude *all* of them, thereby proving

(4.1) THEOREM. *Quadratic extensions K of a number field k are absolutely rigid over k, that is, K is already uniquely determined by its weak decomposition law.*

In view of Jehne's results mentioned above, among Galois extensions only 2-extensions could possibly be absolutely rigid. Hence the next interesting case are the quartic Galois extensions. Concerning these, Praeger proved the following group theoretical result.

(4.2) THEOREM (Praeger [19]). *Let G be a finite group, H a normal subgroup of index 4 and U a maximal subgroup of H with*

$$(*) \qquad U_G := \bigcap_{\sigma \in G} U^\sigma = \{1\} \quad \textit{and} \quad U^G = H^G = H.$$

Then G is a semidirect product of the elementary abelian group $A = C_3 \times C_3$ of order 9 with the cyclic or quaternion group of order 8, and A is contained in H.

The general linear group $\mathrm{GL}_2(3)$ of order 48 contains as subgroups of order 8 three conjugate cyclic, three conjugate dihedral and one quaternion group. Of these, the cyclic and the quaternion group operate transitively on the cyclic subgroups of A. This leads to the fact that the groups G mentioned in the theorem do in fact have subgroups U and H with property $(*)$. From this one easily deduces

(4.3) REMARK. (a) There exist cyclic and biquadratic Galois quartic extensions $L|k$ with the same weak decomposition law as some field $L' \supset L$ of degree 12. Especially these quartic fields L are not absolutely rigid. (b) There exist dihedral extensions of $K|k$ of degree 8 with the same weak decomposition law as some field $K' \supset K$ of degree 24.

PROOF. (a) The possible groups G mentioned in (4.2) are solvable, and hence they occur as Galois groups of extensions $N|k$ (see the front piece of Figure 1). The fact that the corresponding group of order 8 acts transitively on the cyclic subgroups of A means that M (the fixed field of A) has the same weak decomposition law as M' (the field fixed by any of these cyclic subgroups). The subgroups H and U mentioned in (4.2) correspond to the fields L (respectively L'), which also have the same weak decomposition law. The Galois group $G(L|k)$ is a quotient of order 4 of $G(M|k) = G/A$, the cyclic or the quaternion group of order 8. Hence both cyclic and biquadratic extensions $L|k$ occur.

https://doi.org/10.1017/S1446788700034182 Published online by Cambridge University Press

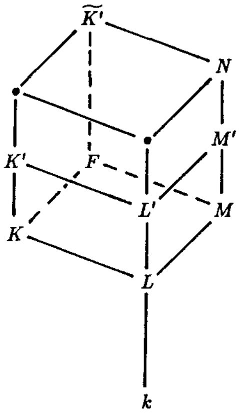

FIGURE 1

(b) It was already well known (Jehne [10]) that the statement of (b) is true even for *any* cyclic or quaternion extension of degree 8, since any such extension $M|k$ can be embedded into an extension $N|k$ with the corresponding group G mentioned in (4.2). For the dihedral group this proof did not work.

To prove (b) we start with a Galois extension $F|k$ with Galois group the unique group of order 16 having as quotients the dihedral *and* the quaternion group of order 8. Let $L|k$ be the extension of degree 4 contained in the quaternion subfield $M \subset F$. Then according to the proof of (a) there exists an extension $L' \supset L$ of degree 12 with the same weak decomposition law as L. Now one easily sees that L must also lie inside the dihedral subfield $K \subset F$ and hence $K' := L'K$ is an extension of degree 24 with the same weak decomposition law as K.

The main result of this section is the following complete classification of all absolutely rigid Galois quartic extensions $K|k$. The given description is explicit, so that one can check for a given Galois quartic number field whether it is absolutely rigid or not.

(4.4) THEOREM. *Let k be a number field, $L|k$ a Galois quartic extension. Then the following statements are equivalent:*

(i) *L is absolutely rigid over k;*

(ii) *$L|k$ is cyclic and -1 is not a norm in $L|k$ or $L = k(\sqrt{a}, \sqrt{b})$ is a biquadratic extension of k and the quadratic form $aX^2 + bY^2 + abZ^2$ is not k-isomorphic to $X^2 + Y^2 + Z^2$.*

PROOF. Let $L|k$ be *cyclic* and assume that -1 is a norm from L. By class field theory we know (see, for example, Artin and Tate [1, Chapter 10, Corollary 2 to Theorem 6]) that in this case $L|k$ may be embedded into a cyclic extension $M|k$ of degree 8. But then the proof of (4.3) applies and we find a field $L' \supset L$ with the same weak decomposition law as L, and hence L is not absolutely rigid. Now let us assume that $L|k$ is cyclic but not absolutely rigid. Since $L|k$ is Galois, any field L' with the same weak decomposition law as L contains L (theorem of Bauer [3], following immediately from (1.4)). Taking $L' \supset L$ minimal with the same weak decomposition law as L and $G = G(N|k)$, the Galois group of the normal closure N of $L'|k$, then Theorem (1.4) shows that the assumptions of (4.2) are satisfied with $H = G(N|L)$ and $U = G(N|L')$. Hence the group G is a semidirect product $A{\cdot}\mathcal{G}$ of $A = C_3 \times C_3$ with $\mathcal{G} = C_8$ or $\mathcal{G} = Q_8$. Since A is contained in H we see that the cyclic group $G(L|k) = G/H$ is a quotient of $\mathcal{G}$, which excludes $\mathcal{G} = Q_8$. But this means that $L|k$ may be embedded into a cyclic extension $M|k$ of degree 8, which is only possible (see Artin and Tate [1]) if -1 is a norm from L.

If in the *biquadratic* case the quadratic form $aX^2 + bY^2 + abZ^2$ is k-isomorphic to $X^2+Y^2+Z^2$, then (see, for example, Serre [23, §3.2, Exemple]) the field $L = k(\sqrt{a}, \sqrt{b})$ is contained in a quaternion extension $M|k$, and again the proof of (4.3) shows the existence of a proper extension field $L' \supset L$ with the same weak decomposition law as L, that is, L is not absolutely rigid. If, on the other hand, L is not absolutely rigid and $L' \neq L$ has the same weak decomposition law as L, then we show, as in the cyclic case, that L is contained in a cyclic or quaternion extension $M|k$ of degree 8. This time $M|k$ has to be quaternion, since $L|k$ is not cyclic. But this implies ([23]) that $aX^2 + bY^2 + abZ^2$ is k-isomorphic to $X^2 + Y^2 + Z^2$.

The conditions of (ii) are of purely local nature because of Hasse's local-global-principle for norms in cyclic extensions (see, for example, Neukirch [16, Chapter IV, Corollary (5.2)]) respectively for quadratic forms (Theorem of Hasse and Minkowski, see for example, O'Meara [17, Chapter VI, 66:4]).

When the ground field k is $\mathbb{Q}$, then these conditions may be easily checked, for example, in the biquadratic case in terms of the sign of a, $b (\in \mathbb{Z})$ and the Legendre symbols (a/p), (b/p) (p prime):

(4.5) COROLLARY. *The following Galois number fields of degree* 4 *are absolutely rigid over* $\mathbb{Q}$, *that is, already determined by their weak decomposition law:*

(1) *all imaginary Galois quartic fields;*

(2) *all biquadratic extensions* L *with quadratic subfields* $\mathbb{Q}(\sqrt{D_i})$ $(i = 1, 2, 3)$, $D_i \in \mathbb{Z}$ *squarefree and at least one* $D_i \equiv -1 \mod 8$;

(3) *exactly those real biquadratic extensions* L *with quadratic subfields* $\mathbb{Q}(\sqrt{D_i})$ $(i = 1, 2, 3, D_i \in \mathbb{N}$ *squarefree*), *for which there exists a prime number* p *and* $i \neq j$ *with* $2 \neq p|D_i$, $p \nmid D_j$, $p \equiv -\frac{D_j}{p} \mod 4$.

PROOF. (1) If $L|\mathbb{Q}$ is imaginary, then the local extension at infinity is $\mathbb{C}|\mathbb{R}$ and -1 is not a norm at the infinite place. Hence the assertion follows in the cyclic case.

If $L = \mathbb{Q}(\sqrt{D_1}, \sqrt{D_2})$ is imaginary biquadratic, then D_1 or D_2 is negative and the quadratic form $D_1X^2 + D_2Y^2 + D_3Z^2$ is not positive definite at the infinite place, and hence not equivalent to $X^2 + Y^2 + Z^2$ over $\mathbb{R}$.

(2) Let $L = \mathbb{Q}(\sqrt{D_1}, \sqrt{D_2})$ with $D_1 \equiv -1 \bmod 8$. If L were not absolutely rigid, then according to (4.4) the quadratic forms $D_1X^2+D_2Y^2+D_3Z^2$ and $X^2 + Y^2 + Z^2$ were $\mathbb{Q}$-isomorphic, and hence they would represent the same numbers over $\mathbb{Q}$. Then especially the number D_1 could be represented as a sum of 3 squares in $\mathbb{Q}$, which however is already impossible mod 8 if $D_1 \equiv -1 \bmod 8$.

(3) According to Theorem (4.4) and the Hasse-Minkowski theorem the field $L = \mathbb{Q}(\sqrt{D_1}, \sqrt{D_2})$ is absolutely rigid if and only if $D_1X^2 + D_2Y^2 + D_3Z^2$ and $X^2 + Y^2 + Z^2$ are not isomorphic locally at some place of $\mathbb{Q}$. Since the D_i are positive, these forms are equivalent over $\mathbb{R}$, and hence there must exist a prime number p such that these forms are not isomorphic over $\mathbb{Q}_p$. Since dimension and discriminant of both forms agree, their Hasse invariants (for example, see O'Meara [17, §66]) must differ at p. Because of the product formula we may assume $p \neq 2$ and hence, for the Hasse invariant H of $D_1X^2 + D_2Y^2 + D_3Z^2$ at some prime $p \neq 2$, we have

$$H = \left(\frac{D_1, D_1}{p}\right)\left(\frac{D_1, D_2}{p}\right)\left(\frac{D_2, D_2}{p}\right) = -1.$$

Using standard computations with the Hilbert symbol (see, for example, Neukirch [16, Chapter III, (5.6)]), we get

$$H = \begin{cases} 1, & p \nmid D_1D_2, \\ \left(\frac{-1}{p}\right)\left(\frac{D_2}{p}\right), & p|D_1,\, p\nmid D_2, \\ \left(\frac{-1}{p}\right)\left(\frac{D_3}{p}\right), & p|D_1,\, p|D_2, \\ \left(\frac{-1}{p}\right)\left(\frac{D_1}{p}\right), & p\nmid D_1,\, p|D_2. \end{cases}$$

This proves assertion (3) of (4.5) because of $p|D_1 \wedge p|D_2 \Rightarrow p \nmid D_3$ and $p \equiv (-1/p) \bmod 4$ for odd prime numbers p.

This corollary shows that in contrast with the quadratic case, in which the result (Theorem (4.1)) is of purely group theoretical nature and applies to all quadratic extensions uniformly, for quartic Galois extensions absolute rigidity is not a purely group theoretical property, but depends on the arithmetic

https://doi.org/10.1017/S1446788700034182 Published online by Cambridge University Press

of the field: for example the real field $\mathbb{Q}(\sqrt{3}, \sqrt{5})$ is absolutely rigid, while $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ is not.

Note added in proof

R. M. Guralnick ('Zeroes of permutation characters with applications to prime splitting', *J. Alg.* **131** (1990), 294–302) has widely extended the list of absolutely rigid extensions of number fields. He proved that any extension $K|k$ of degree n is absolutely rigid if its normal closure $\tilde{K}$ has Galois group A_n $(n > 5)$ or S_n.

The computations of Theorem (3.2) have been extended by C. Moll for any permutation group of degree up to 11 and for the primitive ones up to degree 20.

References

[1] E. Artin and J. Tate, *Class field theory*, (Benjamin, Reading, Mass., 1967).

[2] M. Bauer, 'Über Kreisteilungsgleichungen', *Arch. Math. Phys.* **6** (1904), 220.

[3] M. Bauer, 'Zur Theorie der algebraischen Zahlkörper', *Math. Ann.* **77** (1916), 353–356.

[4] R. Brandl, Letter to W. Jehne, April 22, 1983.

[5] G. Butler and J. McKay, 'The transitive groups of degree up to eleven', *Comm. Algebra* **11** (1983), 863–911.

[6] J. Cassels and A. Fröhlich (eds.), *Algebraic number theory*, (Academic Press, London, New York, 1967).

[7] F. Gaßmann, 'Bemerkungen zur vorstheenden Arbeit von Hurwitz', *Math. Z.* **25** (1926), 665–675.

[8] I. Gerst, 'On the theory of nth power residues and a conjecture of Kronecker', *Acta Arith.* **17** (1970), 121–139.

[9] B. Huppert, *Endliche Gruppen* I, (Springer, Berlin, Heidelberg, New York, 1967).

[10] W. Jehne, 'Kronecker classes of algebraic number fields', *J. Number Theory* **9** (1977), 279–320.

[11] N. Klingen, 'Zahlkörper mit gleicher Primzerlegung', *J. Reine Angew. Math.* **299/300** (1978), 342–384.

[12] N. Klingen, 'Atomare Kronecker-Klassen mit speziellen Galoisgruppen', *Abh. Math. Sem. Univ. Hamburg* **48** (1979), 42–53.

[13] N. Klingen, 'Über schwache quadratische Zerlegungsgesetze', *Comment. Math. Helv.* **55** (1980), 645–651.

[14] K. Komatsu, 'On the adele rings and zeta-functions of algebraic number fields', *Kodai Math. J.* **1** (1978), 394–400.

[15] J. McKay, 'Some remarks on computing Galois groups', *SIAM J. Comput.* **8** (1979), 344–347.

[16] J. Neukirch, *Class field theory*, (Grundlehren Math. Wiss. 280, Springer, Berlin, Heidelberg, New York, Tokyo, 1986).

https://doi.org/10.1017/S1446788700034182 Published online by Cambridge University Press

[17] O. T. O'Meara, *Introduction to quadratic forms*, (Grundlehren Math. Wiss. vol. 117, Springer-Verlag, Göttingen, Heidelberg, 1963).

[18] R. Perlis, 'On the equation $\zeta_K(s) = \zeta_{K'}(s)$', *J. Number Theory* **9** (1977), 342–360.

[19] C. E. Praeger, 'Covering subgroups of groups and Kronecker classes of fields', *J. Algebra*, **118** (1988), 455–463.

[20] ——, 'Kronecker classes of field extensions of small degree', *J. Austral. Math. Soc. Ser. A* **50** (1991), 297–315.

[21] J. Saxl, 'On a question of W. Jehne concerning covering subgroups of groups and Kronecker classes of fields', *J. London Math. Soc.*, to appear.

[22] A. Schinzel, 'On a theorem of Bauer and some of its applications', *Acta Arith.* **11** (1966), 333–344.

[23] J.-P. Serre, 'L'invariant de Witt de la forme $Tr(x^2)$', *Comment. Math. Helv.* **59** (1984), 651–676.

[24] W. Trinks, *Arithmetisch ähnliche Körper*, (Diplomarbeit, Karlsruhe, 1969).

Mathematiches Institut
Universität zu Köln
Weyertal 86-90
D 5000 Köln 41
Germany

https://doi.org/10.1017/S1446788700034182 Published online by Cambridge University Press