ISRAEL JOURNAL OF MATHEMATICS 84 (1993), 89–96

ON EQUIVALENT NUMBER FIELDS WITH SPECIAL GALOIS GROUPS

BY

MANFRED LOCHTER

Universität des Saarlandes, FB 9 Mathematik
66041 Saarbrücken, Germany

ABSTRACT

In [12] and [13] Jack Sonn has introduced and studied a new notion of equivalence for number fields. In this note we show that "almost all" (cf. [14]) pairs of equivalent number fields are conjugate over $\mathbb{Q}$, and we study equivalence classes of fields of prime degree.

Let K be a field, G a finite group. G is called K-**admissible** iff there exists a finite dimensional K-central division algebra D which is a crossed product for G. Two number fields K and L are called **(Sonn)-equivalent** iff the set of K-admissible finite groups and the set of L-admissible finite groups coincide. The following theorem was proved in [12]:

THEOREM 1: *Let K and L be equivalent number fields. Then K and L have the same normal closure over $\mathbb{Q}$.*

Let K be a number field and p a prime. We say p has **decomposition type** $(f_1, \ldots, f_r)$ iff p has exactly r prime divisors of degrees $f_1 \geq f_2 \geq \cdots \geq f_r$ in K. Let $N|\mathbb{Q}$ be a Galois extension containing K and $\mathcal{P}$ be any divisor of p in N. The group $G = G(N|\mathbb{Q})$ acts on the left cosets of $U = G(N|K)$ in G and it is well known (see [1] or [6, Lemma 1]) that for unramified $\mathcal{P}$ the following two conditions are equivalent:

(a) p has decomposition type $(f_1, \ldots, f_r)$ in K.

(b) The Frobenius automorphism $\sigma = F_{N|\mathbb{Q}}(\mathcal{P})$ acts on the left cosets of U as a product of r disjoint cycles of lengths $f_1 \geq f_2 \geq \cdots \geq f_r$ (the **cycle type** of σ is $(f_1, \ldots, f_r)$).

Received August 31, 1992 and in revised form March 9, 1993

THEOREM 2: *Let K and L be equivalent number fields. Let N be the common normal closure of K and L over $\mathbb{Q}$ and let U, $U' \subset G := G(N|\mathbb{Q})$ be the respective fixed groups. Let $\sigma \in G$ act on G/U and on G/U' and let $(f_1, \ldots, f_r)$ and $(f'_1, \ldots, f'_s)$ be the respective cycle types of σ. Then:*

(a) $r = 1 \Leftrightarrow s = 1$.

(b) *If $r \neq 1$ or $s \neq 1$ then $f_2 = f'_2$.*

(c) *The action of σ on the cosets of U is trivial iff the action of σ on the cosets of U' is trivial.*

The following theorem is a reformulation of Theorem 2 in terms of decomposition types. Note that every $\sigma \in G$ *is* Frobenius automorphism corresponding to an unramified prime.

THEOREM 2': *Let K and L be equivalent number fields. For a prime p which is unramified in $K|\mathbb{Q}$ or in $L|\mathbb{Q}$ with respective decomposition types $(f_1, \ldots, f_r)$ and $(f'_1, \ldots, f'_s)$ we have:*

(a) $r = 1 \Leftrightarrow s = 1$.

(b) *If p is not inert in K or in L, then $f_2 = f'_2$.*

(c) *p splits completely in K iff p splits completely in L.*

Proof: (a) and (b) may easily be read off the proof of Theorem 1 in [12]. (c) is a consequence of the fact that two number fields K and L have the same normal closure over $\mathbb{Q}$ iff the sets $S(K|\mathbb{Q})$ of primes splitting completely in $K|\mathbb{Q}$ and $S(L|\mathbb{Q})$ coincide up to a finite number of ramified exceptions. ∎

Another fundamental equivalence relation for number fields was introduced and intensively studied by W. Jehne [5]. Two extensions $K|k$ and $L|k$ of number fields are called **Kronecker equivalent** over k ($K \sim_k L$), iff the **Kronecker sets** $D(K|k)$ of finite primes of k, which have a divisor of first degree in K and $D(L|k)$ coincide up to at most finitely many exceptions (which according to [6] do not exist). It is interesting to see, that Kronecker equivalent fields share the property (a) and weakened versions of the properties (b) and (c) of the following Remark 3. It is not even necessary to exclude ramified primes of the ground field k ([9]). On the other hand Kronecker equivalent fields need not have the same normal closure. Let $L|\mathbb{Q}$ be normal and $K|\mathbb{Q}$ be arbitrary. If K and L are equivalent then $K \subset L$. If K and L are Kronecker equivalent, then $K \supset L$. So Kronecker equivalence and equivalence are dual in some sense.

Two extensions $K|k$ and $L|k$ of algebraic number fields are called **arithmetically equivalent** over k (see [11], [6]) iff (almost) all primes of k have the same decomposition type in K and in L. K and L are arithmetically equivalent over $\mathbb{Q}$ iff their Dedekind zetafunctions coincide. Arithmetically equivalent fields are obviously Kronecker equivalent. Theorem 5 shows that equivalent fields of prime degree are arithmetically equivalent.

Remark 3: Let K and L be equivalent number fields with common normal closure N over $\mathbb{Q}$. For a prime p, unramified in $N|\mathbb{Q}$, with decomposition types $(f_1,\ldots,f_r)$ in K and $(f'_1,\ldots,f'_s)$ in L we have:

(a) Let $i\in\{1,\ldots,r\}$. Then:

$$\forall_{j\neq i}\gcd(f_i,f_j)=1 \implies \exists_{j\in\{1,\ldots,s\}} f_i|f'_j.$$

(b) If p has decomposition type $(f_1,\ldots,f_{r_1},1,\ldots,1)$ in K with $\gcd(f_i,f_j)=1$ $(i\neq j)$ then p has decomposition type $(f_1,\ldots,f_{r_1},1,\ldots,1)$ in L. Only the number of occurrences of the residue degree 1 may be different.

(c) Let p be inert in $K|\mathbb{Q}$. Then the degrees $(K\colon\mathbb{Q})$ and $(L\colon\mathbb{Q})$ coincide.

Proof: Let $G=G(N|\mathbb{Q}), U=G(N|K), U'=G(N|L)$ and $\sigma=F_{N|\mathbb{Q}}(\mathcal{P})$ for a prime divisor of p in N. We consider

$$\tau := \sigma^{f_1\cdots\hat{f_i}\cdots f_r}.$$

(a) $\operatorname{ord}(\sigma)=\operatorname{lcm}(f_1,\ldots,f_r)$ implies $\operatorname{ord}(\tau)=f_i$. τ is Frobenius automorphism, corresponding to an unramified prime $\tilde{p}$. The decomposition type of $\tilde{p}$ in K is $(f_i,1,\ldots,1)$. By Theorem 1, G acts faithfully on G/U *and* on G/U'. Now Theorem 2 implies that $\tilde{p}$ has a decomposition type of form $(f_i,1,\ldots,1)$ in L, too.

(b) Similarly one deduces

$$\forall_{\substack{i\neq j\\ i,j\in\{1,\ldots,r\}}}\gcd(f_i,f_j)=1 \implies \forall_{\substack{i\neq j\\ i,j\in\{1,\ldots,s\}}}\gcd(f'_i,f'_j)=1.$$

Now (b) follows from $\operatorname{lcm}(f_1,\ldots,f_r)=\operatorname{lcm}(f'_1,\ldots,f'_s)$.

(c) follows from Theorem 2(a). ∎

The following example will be used later:

Example 4: Let K be an algebraic number field of degree n over the rationals with normal closure $\tilde{K}|\mathbb{Q}$ and

$$G(\tilde{K}|\mathbb{Q}) = S_n \qquad \text{or} \qquad G(\tilde{K}|\mathbb{Q}) = A_n \quad \text{with } n \text{ odd.}$$

Then every field L, equivalent to K, has degree n over $\mathbb{Q}$.

Proof: Follows from Remark 3(c). ∎

We now examine equivalence classes of fields of prime degree.

THEOREM 5: *Let K be a number field of prime degree p over $\mathbb{Q}$ and L be a field of arbitrary degree which is equivalent to K. Then:*

(a) $(K\colon \mathbb{Q}) = (L\colon \mathbb{Q})$.

(b) *K and L are arithmetically equivalent over $\mathbb{Q}$.*

(c) *If $G = G(\tilde{K}|\mathbb{Q})$ is solvable, then K and L are conjugate over $\mathbb{Q}$.*

(d) *The degrees p and groups G for which non-trivial equivalence is possible are known by [2].*

(e) *In any case we have for $i \in \mathbb{N}$: $K_i(\mathcal{O}_K)_p \simeq K_i(\mathcal{O}_L)_p$ where $K_i(\mathcal{O}_K)_p$ denotes the p-primary part of the i-th Quillen K-group of the ring of integers of K. In particular, $Cl(\mathcal{O}_K)_p \simeq Cl(\mathcal{O}_L)_p$. Moreover, the unit groups of K and L are isomorphic.*

Proof: (a) Let $N|\mathbb{Q}$ be the common normal closure of K and L. Let $G = G(N|\mathbb{Q})$, $U = G(N|K)$ and $U' = G(N|L)$. G is a subgroup of the symmetric group S_p, hence p does not divide $\#U$. We choose an element $\sigma \in G$ of order p. σ acts on G/U without fixed points as a cycle of length p. Now (a) follows from Theorem 3(c).

(b) By (a) the Sylow p-subgroups of U and U' are conjugate. Therefore (b) follows from [3, Theorem 2.1].

(c) U and U' are $\{p\}'$-Hall subgroups, hence conjugate.

(d) See [2].

(e) It is well known that for arithmetically equivalent number fields the unit groups coincide ([11]). The rest follows from [8]. ∎

Now we consider fields of low degree:

THEOREM 6: *Let K be a number field of degree $(K\colon \mathbb{Q}) \leq 5$. Then every field L which is equivalent to K is conjugate to K.*

Proof: It is well known that arithmetically equivalent fields of degree less than 7 are conjugate ([11]). Because of Theorem 5 we only have to look at the case $(K\colon \mathbb{Q}) = 4$. The group $G = G(\tilde{K}|\mathbb{Q}) = G(\tilde{L}|\mathbb{Q})$ is a subgroup of the symmetric group S_4. The case $G = S_4$ will be treated in the next theorem, so suppose $\#G \in \{4, 8, 12\}$. Theorem 5 implies $(L\colon \mathbb{Q}) \geq 4$, consequently $(L\colon \mathbb{Q}) \in \{4, 6, 8, 12\}$, and $(L\colon \mathbb{Q})$ divides $\#G$.

$\underline{\#G = 4}$: K and L are conjugate by Theorem 1.

$\underline{\#G = 8}$: Then we have $(L\colon \mathbb{Q}) \in \{4, 8\}$. Let p be any prime which is unramified in $\tilde{K}|\mathbb{Q}$ and M be any subfield of $\tilde{K}|\mathbb{Q}$ of degree 4. The possible decomposition types of p in M are

$$(4), \quad (2,2), \quad (2,1,1), \quad (1,1,1,1). \tag{1}$$

$(L\colon \mathbb{Q}) = 4$: Theorem 2 together with (1) implies, that K and L are arithmetically equivalent, hence conjugate.

$(L\colon \mathbb{Q}) = 8$: From (1) and Theorem 2 we conclude $D(K|\mathbb{Q}) \subset D(L|\mathbb{Q})$ up to at most finitely many exceptions. Now the Theorem of M. Bauer (see [10]) yields the contradiction $K \supset L$.

$\underline{\#G = 12}$: We have $(L\colon \mathbb{Q}) \in \{4, 6, 12\}$. In this case the possible decomposition types of unramified primes in one of the subfields of degree four of $\tilde{K}|\mathbb{Q}$ are

$$(4), \quad (3,1), \quad (2,2), \quad (2,1,1), \quad (1,1,1,1). \tag{2}$$

$(L\colon \mathbb{Q}) = 4$: Again K and L are arithmetically equivalent.

$(L\colon \mathbb{Q}) \in \{6, 12\}$: The group $U = G(\tilde{K}|K) = \langle\sigma\rangle$ is cyclic of order three and σ acts on G/U as a 3-cycle. By Theorem 2(b), σ fixes one coset of U' in G, hence σ is contained in a subgroup conjugate to U' and we derive the contradiction $3|\#U'$. ∎

Now we are ready to prove our main theorem, which shows that "almost all" (cf. [14]) equivalent fields are conjugate. In the course of the proof we shall use ideas of N. Klingen [7].

THEOREM 7: *Let K be a number field with $(K\colon \mathbb{Q}) = n$ and $G(\tilde{K}|\mathbb{Q}) = S_n$ or $G(\tilde{K}|\mathbb{Q}) = A_n$. Then every field L which is equivalent to K is conjugate to K.*

Proof: Let $G = G(\tilde{K}|\mathbb{Q})$, $U = G(\tilde{K}|K), U' = G(\tilde{K}|L)$. We regard G as a subgroup of the symmetric group $S_{(G\colon U)} = S_n$ and identify the set G/U with $\{1,\ldots,n\}$. Without loss of generality we may assume $U = \mathrm{Fix}_G(n)$. We consider three cases:

(I) $G = S_n$ $\quad n \geq 4$.

(II) $G = A_n$ $\quad n \geq 6,\quad n$ even.

(III) $G = A_n$ $\quad n \geq 7,\quad n$ odd.

CASE (I): By Example 4 we have $(G\colon U) = (G\colon U')$. By Huppert ([4, p.175]) our assertion is true for $n \neq 6$. But it is possible to give a simple proof which works in all cases. For this purpose we first establish the following two facts:

$$\text{(3)}\qquad U' \text{ contains a } (n-1)\text{-cycle } \sigma = (a_1,\ldots,a_{n-1}).$$

$$\text{(4)}\qquad U' \text{ contains a transposition } \tau = (c_1,c_2).$$

(3): $G = S_n$ contains σ_1, which acts on G/U as a $(n-1)$-cycle: The cycle type of σ_1 is $(n-1,1)$. The cycle type of σ_1 viewed as element of $S_{G/U'}$ is also $(n-1,1)$ by Theorem 2(b). There exists $\sigma \in G$ which is conjugate to σ_1 and contained in U'. Obviously σ is a $(n-1)$-cycle.

(4) may be shown similarly.

Now we define a_n by $\{1,\ldots,n\} = \{a_1,\ldots,a_n\}$ and take $\eta \in U'$ with $\eta(a_n) = a_j \in \{a_1,\ldots,a_{n-1}\}$. $\mathrm{Fix}_{U'}(a_n)$ acts transitively on $\{a_1,\ldots,a_{n-1}\}$ and U' acts transitively on $\{a_1,\ldots,a_n\}$: U' is 2-transitive on $\{a_1,\ldots,a_n\}$, hence primitive. Now [4, II 4.5] and (4) give the contradiction $U' = S_n$. Hence we have $U' = \mathrm{Fix}_{S_n}(a_n)$.

CASE (II): We show:

$$\text{(5)}\qquad U' \neq A_n$$

$$\text{(6)}\qquad U' \text{ contains a } (n-1)\text{-cycle } \sigma = (a_1,\ldots,a_{n-1}).$$

$$\text{(7)}\qquad U' \text{ contains a 3-cycle } \tau = (b_1,b_2,b_3).$$

(5) follows from Theorem 1. A_n contains a $(n-1)$-cycle because $n-1$ is odd.
(6) can be shown similarly to (3). (7) is now clear.

Let again a_n be defined by $\{a_1,\ldots,a_n\} = \{1,\ldots,n\}$. We distinguish two cases:

(a): $U' \subset \mathrm{Fix}_{A_n}(a_n)$. Without loss of generality we may assume $U' \subset U$. By (7) and Theorem 2 there exists $\tau \in U'$, which acts as 3-cycle on G/U *and* on G/U'. This is only possible if $U = U'$.

(b): $U' \not\subset \mathrm{Fix}_{A_n}(a_n)$. U' acts transitively on $\{a_1, \ldots, a_n\} = \{1, \ldots, n\}$. By (6) it follows, that the action of U' on $\{a_1, \ldots, a_n\}$ is primitive. (7) and [4, II 4.5] yield $U' \supset A_n$. Contradiction to (5).

Case (III): Again we know $\#U = \#U'$ and show:

$$U' \text{ contains a product of disjoint } \frac{n-1}{2}\text{-cycles}$$

(8) $$\sigma = (a_1, \ldots, a_{\frac{n-1}{2}})(a_{\frac{n-1}{2}+1}, \ldots, a_{n-1})$$

(9) $$U' \text{ contains a } (n-2)\text{-cycle } \tau = (b_1, \ldots, b_{n-2}).$$

(10) $$U' \text{ contains a 3-cycle } \rho = (c_1, c_2, c_3).$$

It is only necessary to show (8). $U = \mathrm{Fix}_{A_n}(n)$ contains a product of disjoint $\frac{n-1}{2}$-cycles, for example

$$\sigma_1 := \left(1, \ldots, \frac{n-1}{2}\right)\left(\frac{n-1}{2} + 1, \ldots, n-1\right).$$

σ_1 viewed as element of $S_{G/U}$ has cycle type $(\frac{n-1}{2}, \frac{n-1}{2}, 1)$, σ_1 viewed as element of $S_{G/U'}$ has cycle type

$$(f'_1, f'_2, \ldots, f'_s) \qquad \text{with } s \geq 2$$

under the restrictions

Theorem 2 $$f'_2 = \frac{n-1}{2}$$

$$f'_1 \geq f'_2$$

Example 4 $$\sum_{i=1}^{s} f'_i = n$$

Theorem 1 $$\mathrm{lcm}(f'_1, \ldots, f'_s) = \frac{n-1}{2} = \mathrm{ord}(\sigma_1).$$

These restrictions allow only $(f'_1, \ldots, f'_s) = (\frac{n-1}{2}, \frac{n-1}{2}, 1)$. U' contains an element σ_1, conjugate to σ, of the desired form. From $\frac{n-1}{2} \leq 2 \Leftrightarrow n \leq 5$ we conclude $\{b_1, \ldots, b_{n-2}\} \cap \{a_1, \ldots, a_{\frac{n-1}{2}}\} \neq \emptyset$, and $\{b_1, \ldots, b_{n-2}\} \cap \{a_{\frac{n-1}{2}+1}, \ldots, a_{n-1}\} \neq \emptyset$, thus

(11) $$U' \quad \text{acts transitively on} \quad \{a_1, \ldots, a_{n-1}\} \cup \{b_1, \ldots, b_{n-2}\}$$

Again we have to distinguish two different cases:

(a): *U' does not act transitively on $\{1,\dots,n\}$*. Then (11) gives $\{b_1,\dots,b_{n-2}\} \subset \{a_1,\dots,a_{n-1}\}$ and $U' \subset \mathrm{Fix}_{A_n}(a_n)$. But we already know $\#U' = \#U$; so U and U' are conjugate.

(b): *U' acts transitively on $\{1,\dots,n\}$*. σ is contained in $\mathrm{Fix}_{U'}(a_n) = V$. We define b_{n-1} and b_n by $\{b_1,\dots,b_n\} = \{1,\dots,n\}$ and choose $\alpha \in U'$ with $\alpha(b_n) = a_n$. U' contains the $(n-2)$-cycle

$$(b'_1,\dots,b'_{n-2}) = \alpha\tau\alpha^{-1} = (\alpha(b_1),\dots,\alpha(b_{n-2})),$$

which also lies in the subgroup V, which acts transitively on $\{a_1,\dots,a_{n-1}\}$ (cf. (11)). From Huppert [4, II 4.5] we derive the contradiction $U' \supset A_n$.

This completes the proof of Theorem 7. ∎

References

[1] E. Artin, *Über die Zetafunktionen gewisser algebraischer Zahlkörper*, Math. Ann. **89** (1923), 147–156.

[2] W. Feit, *Some consequences of the classification of finite simple groups*, Proceedings of Symposia in Pure Mathematics **37** (1980), 175–181.

[3] R. Guralnick and D. Wales, *Subgroups inducing the same permutation representation II*, J. Alg. **96** (1985), 94–113.

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

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

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

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

[8] K. Komatsu, *Einige Bemerkungen über Dedekindsche Zetafunktionen und K-Gruppe*, Arch. Math. **54** (1990), 164–165.

[9] M. Lochter, *New characterizations of Kronecker equivalence*, submitted.

[10] J. Neukirch, *Class Field Theory*, Springer, Berlin, 1986.

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

[12] J. Sonn, *On equivalence of number fields*, Isr. J. Math. **52** (1985), 239–244.

[13] J. Sonn, Correction to "*On equivalence of number fields*", Isr. J. Math. **71** (1990), 379.

[14] B. L. van der Waerden, *Zur Seltenheit der Gleichungen mit Affekt*, Math. Ann. **109** (1934), 13–16.