ACTA ARITHMETICA
105.1 (2002)

Linear forms and arithmetic equivalence

by

Marius Somodi (Cedar Falls, IA)

1. Introduction. One of the problems in algebraic number theory is to characterize number fields by splitting properties of prime ideals from the ground field. In the study of this problem various types of equivalence between number fields have been introduced.

To fix the notations, let p be any rational prime, and let K and K' be two number fields. Let $f_1(p) \le \ldots \le f_r(p)$ be the inertial degrees of p in K and $f'_1(p) \le \ldots \le f'_s(p)$ be the inertial degrees of p in K'. Let $g_K(p) = r$ and $g_{K'}(p) = s$ be the number of distinct prime divisors of p in K and K' respectively. For any rational prime p and any $l \ge 1$, let $k_l(p)$ be the number of prime factors of p in K that have the inertial degree equal to l and $k'_l(p)$ be the number of prime factors of p in K' that have the inertial degree equal to l. Clearly, for every prime p, only finitely many numbers $k_l(p)$ and $k'_l(p)$ are nonzero.

K and K' are called:

(A) *arithmetically equivalent* if for almost all rational primes p, $g_K(p) = g_{K'}(p)$ and $f_i(p) = f'_i(p)$ for all $i = 1, \ldots, r$ (as usual, "for almost all" means for all except possibly a set of primes of Dirichlet density zero);

(S) *split equivalent* if for almost all rational primes p, $g_K(p) = g_{K'}(p)$;

(SK) *super Kronecker equivalent* if for almost all rational primes p, $k_1(p) = k'_1(p)$;

(K) *Kronecker equivalent* if for almost all rational primes p, $k_1(p) > 0$ iff $k'_1(p) > 0$;

(WK) *weakly Kronecker equivalent* if for almost all rational primes p,

$$\gcd(f_1(p), \ldots, f_r(p)) = 1 \quad \text{iff} \quad \gcd(f'_1(p), \ldots, f'_r(p)) = 1.$$

Here are the logical connections between these concepts ([2–5, 8]):

$$(\mathrm{SK}) \Leftrightarrow (\mathrm{S}) \Leftrightarrow (\mathrm{A}) \Rightarrow (\mathrm{K}) \Rightarrow (\mathrm{WK})$$

(the last two implications cannot be reversed).

2000 *Mathematics Subject Classification*: Primary 11R04.

In this paper we will define a more general type of equivalence between two number fields, called *linear equivalence*. Arithmetic equivalence of two number fields always implies linear equivalence. However the two concepts are equivalent under some special circumstances that will be investigated in this paper. We will see that both split equivalence and super Kronecker equivalence are particular cases of linear equivalence. By investigating the connection between linear equivalence and arithmetic equivalence we also present a unified proof for the logical equivalence between split, super Kronecker, and arithmetic equivalence. As concerns Kronecker and weak Kronecker equivalences, we are not aware of a general relation with linear equivalence (except for the particular situation when linear equivalence implies arithmetic equivalence and thus Kronecker and weak Kronecker equivalence).

There are other characterizations of arithmetic equivalence (involving Dedekind zeta functions or group representations). Since we will not use them, we refer the interested reader to [3, 6, 7]. We will mention though that arithmetically equivalent number fields have the same zeta function. The aim of this paper is to introduce the more general concept of linear equivalence and to present a new and unified proof for the known results that both super Kronecker and split equivalence imply arithmetic equivalence.

2. The main result. Let K and K' be two number fields, and let $n = [K : \mathbb{Q}]$, $n' = [K' : \mathbb{Q}]$. Without loss of generality we can assume $n' \leq n$. Throughout the paper μ will denote the Möbius function.

Let $F = \sum_{l=1}^{\infty} a_l X_l$ be an infinite-dimensional linear form, where the coefficients $a_1, a_2, \ldots$ are integers. The form F induces a homomorphism of abelian groups

$$F : \mathbb{Z} \oplus \mathbb{Z} \oplus \ldots \to \mathbb{Z}.$$

Let

$$F_K(p) = F(k_1(p), k_2(p), \ldots), \qquad F_{K'}(p) = F(k'_1(p), k'_2(p), \ldots),$$

where p is any rational prime.

Definition 2.1. We say that K and K' are *F-linearly equivalent* (or simply *linearly equivalent*) if, for almost all p, $F_K(p) = F_{K'}(p)$.

The main theorem will show that linear equivalence can be as strong as arithmetic equivalence if the coefficients of the linear form satisfy the following conditions:

$$\sum_{d \mid m} \mu(d) \, \frac{m}{d} \, a_d \neq 0, \qquad \forall m = 1, \ldots, c, \tag{1}$$

for some integral constant $c \geq 2$.

Note that there are linear forms that satisfy the above conditions: for instance one can take $a_1 = 1$ and $a_i = 0$ for all $i \geq 2$. This form satisfies the conditions (1) for any $c \geq 2$.

Here is the main result:

THEOREM 2.2. *Fix an integer $c \geq 2$. Algebraic number fields K and K' of degrees over $\mathbb{Q}$ at most c are arithmetically equivalent if and only if they are linearly equivalent through a linear form F that satisfies* (1).

Proof. Obviously, arithmetic equivalence implies F-linear equivalence for any form F (in particular for any form that satisfies (1)) since any rational prime has the same sequence of f_i's in K and K'.

Suppose now that K and K' are F-linearly equivalent, where the coefficients of F satisfy (1). Let

$$\Gamma = \{p \mid F_K(p) = F_{K'}(p)\}.$$

Then the set of primes outside Γ has Dirichlet density zero.

Let N be a normal extension of $\mathbb{Q}$ that contains K and K'. Let $G = \mathrm{Gal}(N|\mathbb{Q})$, $H = \mathrm{Gal}(N|K)$ and $H' = \mathrm{Gal}(N|K')$. We shall prove that almost all rational primes have the same list of f_i's in K and K'. Fix $g \in G$ and denote by $o = o(g)$ the order of g.

By the Chebotarev density theorem, the set of rational primes that are unramified in N and have the Frobenius automorphism in N equal to g has a positive density. So there exists a prime $p_1 \in \Gamma$ unramified in N whose Frobenius automorphism in N is g. The group G acts by left translations on the left cosets xH, $x \in G$. This action induces a group homomorphism $\Psi : G \to S_n$. Let $\tau = \Psi(g)$. Then the cycle structure of τ describes the splitting of p_1 in K: the splitting number of p_1 in K is the number of disjoint cycles of τ, and the sequence of inertial degrees of primes in K lying over p_1 is the sequence of lengths of disjoint cycles in τ (see [1, Proposition 2.8, p. 101]). Similarly, the action of G on the left cosets xH', $x \in G$, induces a group homomorphism $\Psi' : G \to S_{n'}$. Let $\tau' = \Psi'(g)$.

Then, with our notations, $k_l(p_1)$ = the number of disjoint l-cycles of τ and $k'_l(p_1)$ = the number of disjoint l-cycles of τ', for any l. We know that $F_K(p_1) = F_{K'}(p_1)$, so that

$$\sum_{l=1}^{o} a_l(k_l(p_1) - k'_l(p_1)) = 0. \tag{2}$$

A particular situation is when $g = e$. In this case (2) implies $n = n'$.

By the Chebotarev density theorem, the set of rational primes that are unramified in N and have the Frobenius automorphism in N equal to g^2 has a positive density. So there exists a prime $p_2 \in \Gamma$ unramified in N whose Frobenius automorphism in N is g^2. Since Ψ and Ψ' are group homomorphisms, the permutations associated to g^2 by these two maps are τ^2 and τ'^2

respectively. If $(k_1, k_2, \ldots)$ is the cycle structure of τ, then $(k_1+2k_2, 2k_4, \ldots)$ is the cycle structure of τ^2 (as every 2-cycle in τ gives two 1-cycles in τ^2, every 4-cycle in τ gives two 2-cycles in τ^2, etc.), and similarly for τ'^2. Since $p_2 \in \Gamma$, we have $F_K(p_2) = F_{K'}(p_2)$, so that

$$\sum_{l=1}^{o} a_l(k_l(p_2) - k'_l(p_2)) = 0. \tag{3}$$

We continue to apply the same technique for $g^3, g^4, \ldots, g^o = e$. In this way, we get a linear homogeneous system of equations with variables $k_1 - k'_1$, $k_2 - k'_2, \ldots, k_o - k'_o$. If $o > c$ then

$$k_{c+1} = \ldots = k_o = k'_{c+1} = \ldots = k'_o = 0,$$

hence we can consider the subsystem that consists of the first c equations:

$$\sum_{l=1}^{c} a_l(k_l(p_i) - k'_l(p_i)) = 0, \qquad i = 1, \ldots, c. \tag{4}$$

Let $t = \min\{o, c\}$. The matrix of this system is $B = (b_{i,j})_{1\le i,j\le t}$, where $b_{i,j} = (i,j)a_{j/(i,j)}$; here $(i,j) = \gcd(i,j)$. By using Lemma 2.3 proved below, we find that, under the assumptions from (1), $\det(B) \neq 0$. To see this, let $1 \le m \le t$ and let m' be the largest squarefree divisor of m. Then

$$\sum_{d|m} \mu(d)\,\frac{m}{d}\,a_d = \sum_{d|m'} \mu(d)\,\frac{m}{d}\,a_d.$$

If $q = m/m'$ then

$$\sum_{d|m} \mu(d)\,\frac{m}{d}\,a_d = q\sum_{d|m'} \mu(d)\,\frac{m'}{d}\,a_d.$$

It follows that any factor of the product from Lemma 2.3 is a (nonzero) multiple of a certain expression from (1) with m' a squarefree integer. So the system has only the trivial solution if the conditions (1) are satisfied. Then all the unramified primes $p \in \Gamma$ whose Frobenius automorphism in N is g have the same sequence of f_i's in K and K'. If we repeat this procedure for any $g \in G$ we obtain the arithmetic equivalence of K and K'. ∎

Note that we proved in fact a stronger result: to verify that two number fields of degree at most c are arithmetically equivalent, it is enough to show that they are linearly equivalent via a form F that satisfies (1) where m runs over the set of squarefree integers between 1 and c.

In order to complete the proof we will prove the following lemmas:

Lemma 2.3. *If $B = (b_{i,j})_{1\le i,j\le t}$ is the matrix with*

$$b_{i,j} = \gcd(i,j)a_{j/\gcd(i,j)}, \qquad \forall i,j,$$

then

$$\det(B) = \prod_{m=1}^{t} \sum_{d|m} \mu(d)\, \frac{m}{d}\, a_d.$$

Proof. We transform the matrix B (without changing $\det(B)$) as follows. First subtract the first row from all the others. Then, for any prime $p \le t$, subtract the pth row from rows $2p,\ 3p, \ldots$ At the next step, for any number of the form pq with p and q primes not necessarily distinct, such that $pq \le t$, subtract the pqth row from rows $2pq, 3pq, \ldots$ Continue until no other transformation can be performed. Denote by $C = (c_{i,j})_{1\le i,j\le t}$ the matrix obtained in this way. Note that, after the first transformation, the new matrix has the form

$$\begin{bmatrix} a_1 & a_2 & \ldots \\ 0 & 2a_1 - a_2 & \ldots \\ 0 & 0 & \ldots \\ 0 & 2a_1 - a_2 & \ldots \\ 0 & 0 & \ldots \\ \vdots & \vdots & \ldots \end{bmatrix}.$$

After the second transformation, we obtain

$$\begin{bmatrix} a_1 & a_2 & \ldots \\ 0 & 2a_1 - a_2 & \ldots \\ 0 & 0 & \ldots \\ 0 & 0 & \ldots \\ 0 & 0 & \ldots \\ \vdots & \vdots & \ldots \end{bmatrix}.$$

The particular form of the original matrix B causes that the final matrix is upper triangular (Lemma 2.6). According to Lemma 2.5,

$$c_{m,m} = \sum_{d|m} \mu(d)\, \frac{m}{d}\, a_d,$$

so the claim is proved. ∎

The following basic property of the Möbius function will enable us to complete the proof of Lemma 2.3.

LEMMA 2.4. *If k, m are two integers such that m does not divide k and if $r \mid \gcd(k, m)$ then*

$$\sum_{d|m,\ (d,k)=r} \mu\Big(\frac{m}{d}\Big) = 0.$$

Proof. Note that, under these assumptions, the set of conditions $d \mid m$, $\gcd(d, k) = r$ is equivalent to $r \mid d \mid m$, $\gcd(k, d/r) = 1$.

Denote by u the largest divisor of m/r whose prime factors are divisors of k. Then the conditions $r \mid d \mid m$, $(k, d/r) = 1$ are equivalent to $r \mid d \mid \frac{m}{u}$.

Consequently,

$$\sum_{d|m,\,(d,k)=r}\mu\left(\frac{m}{d}\right)=\sum_{r|d|\frac{m}{u}}\mu\left(\frac{m}{d}\right)=\sum_{d'|\frac{m}{ur}}\mu\left(\frac{m}{d'r}\right)=\sum_{l|\frac{m}{ur}}\mu(ul)=\mu(u)\sum_{l|\frac{m}{ur}}\mu(l).$$

The Möbius function is the reciprocal of the Riemann zeta function as Dirichlet series ([9]). Hence, if $m/(ur)\neq 1$ then the last sum is 0. It is easy to see that, since m does not divide k, $m/(ur)\neq 1$. ■

LEMMA 2.5. *With the notations of Lemma* 2.3,

$$c_{m,k}=\sum_{d|m}\mu\left(\frac{m}{d}\right)(d,k)a_{k/(d,m)},\qquad 1\le m,k\le t.$$

Proof. Fix any $k\in\{1,\dots,t\}$. The transformations applied to B yield

$$c_{m,k}=b_{m,k}-\sum_{d|m,\,d\neq m}c_{d,k}.$$

Then $b_{m,k}=\sum_{d|m}c_{d,k}$, for all m and, by the Möbius inversion formula,

$$c_{m,k}=\sum_{d|m}\mu\left(\frac{m}{d}\right)b_{d,k}=\sum_{d|m}\mu\left(\frac{m}{d}\right)(d,k)a_{k/(d,k)}.\ ■$$

LEMMA 2.6. *With the notations of Lemma* 2.3, *C is an upper triangular matrix.*

Proof. Let $k<m$. By Lemma 2.5,

$$c_{m,k}=\sum_{d|m}\mu\left(\frac{m}{d}\right)(d,k)a_{k/(d,k)}=\sum_{r|k}\sum_{d|m,\,(d,k)=r}\mu(d)ra_{k/r}$$
$$=\sum_{r|k}ra_{k/r}\sum_{d|m,\,(d,k)=r}\mu\left(\frac{m}{d}\right)=0$$

from Lemma 2.4. ■

3. Examples and remarks

1. If F is the null form (i.e. $a_i=0$ for all i) then any two number fields are F-linearly equivalent.

2. Now take $a_l=l$ for all l. Note that if p is a prime unramified in N then $F_K(p)=n$ and $F_{K'}(p)=n'$. So, for this linear form, F-linear equivalence is equivalent to the condition that K and K' have the same degree over $\mathbb{Q}$. This form does not satisfy (1) for $c\geq 2$.

3. Let K and K' be two normal number fields of degree p over $\mathbb{Q}$, where p is a prime integer, and such that K and K' are not arithmetically equivalent. Consider the linear form

$$F(X_1,X_2,\dots)=X_1+pX_p.$$

Then K and K' are F-linearly equivalent, as $F_K(q) = F_{K'}(q) = p$ for any unramified prime q. The coefficients of F do not satisfy (1) for $c \geq p$ so the main result does not apply.

4. Consider the sequence given by $a_1 = 1$, $a_l = 0$ for all $l > 1$. It satisfies (1), hence if $F_K(p) = F_{K'}(p)$ for almost all primes p then by the main theorem the fields are arithmetically equivalent. But $F_K(p) = k_1(p)$, the number of prime divisors of p in K with inertial degree 1, and similarly for K'. For this linear form, F-linear equivalence is equivalent to super Kronecker equivalence. So we proved that arithmetic equivalence is equivalent to super Kronecker equivalence.

5. Finally, consider the sequence given by $a_l = 1$ for all l. We verify that it satisfies (1). Let $m > 1$ be any squarefree integer. Write $m = p_1 \ldots p_r$, with $p_1, \ldots, p_r$ pairwise distinct primes. Note that

$$\sum_{d|m} \mu(d)\,\frac{m}{d} = (-1)^r \Big(1 - \sum_{i=1}^{r} p_i + \sum_{1\leq i<j\leq r} p_i p_j - \ldots\Big).$$

If we consider the polynomial $f(X) = (X - p_1) \ldots (X - p_r)$ then the above sum is equal to $(-1)^r f(1)$. Since $f(1) \neq 0$, the conditions (1) are satisfied.

For this form, F-linear equivalence means split equivalence, so split equivalence is equivalent to arithmetic equivalence.

References

[1] G. Janusz, *Algebraic Number Fields*, Academic Press, 1973.

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

[3] N. Klingen, *Arithmetical Similarities*, Oxford Univ. Press, Oxford, 1998.

[4] M. Lochter, *Weakly Kronecker equivalent number fields*, Acta Arith. 67 (1994), 295–312.

[5] —, *Weakly Kronecker equivalent number fields and global norms*, ibid. 67 (1994), 105–121.

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

[7] —, *On the class number of arithmetically equivalent fields*, ibid. 10 (1978), 489–509.

[8] D. Stuart and R. Perlis, *A new characterization of arithmetic equivalence*, ibid. 53 (1995), 300–308.

[9] H. S. Wilf, *Generatingfunctionology*, Academic Press, 1994.

Department of Mathematics
University of Northern Iowa
Cedar Falls, IA 50614, U.S.A.
E-mail: somodi@math-cs.cns.uni.edu

Received on 17.2.1999
and in revised form on 31.1.2002 (3557)