BULLETIN OF THE POLISH
ACADEMY OF SCIENCES
MATHEMATICS
Vol. 59, No. 3, 2011

On Exceptions in the Brauer–Kuroda Relations

by

Jerzy BROWKIN, Juliusz BRZEZIŃSKI and Kejian XU

Presented by Jerzy KACZOROWSKI

Summary. Let F be a Galois extension of a number field k with the Galois group G. The Brauer–Kuroda theorem gives an expression of the Dedekind zeta function of the field F as a product of zeta functions of some of its subfields containing k, provided the group G is not exceptional. In this paper, we investigate the exceptional groups. In particular, we determine all nilpotent exceptional groups, and give a sufficient condition for a group to be exceptional. We give many examples of nonnilpotent solvable and nonsolvable exceptional groups.

1. Introduction. Let F be a finite Galois extension of a number field k with the Galois group G. R. Brauer [B] and S. Kuroda [K] proved independently some multiplicative relations between the Dedekind zeta functions of some subfields of F. In general, this leads to an expression of the zeta function $\zeta_F(s)$ of F as the product with rational exponents of the zeta functions of some subfields of F. Yet there are some exceptions.

The well known exception is when the group G is cyclic. Then the Brauer–Kuroda relation takes the form $\zeta_k(s) = \zeta_k(s)$, where $\zeta_k(s)$ is the zeta function of the field k. Another exception is when G is the (generalized) quaternion group of order $2^m, m \geq 3$.

In the present paper, we give a sufficient condition for a group G to be exceptional, and we prove that it is necessary in the class of all finite nilpotent groups. Moreover, we give many examples of nonnilpotent exceptional groups.

2010 *Mathematics Subject Classification*: Primary 20D15; Secondary 11R42.
Key words and phrases: exceptional groups, Brauer–Kuroda relations.

DOI: 10.4064/ba59-3-3

2. Brauer–Kuroda relations. Let G be a finite group. For every cyclic subgroup H of G, we define

$$c_G(H) := \frac{1}{(G:H)} \sum_{\substack{H^* \text{ cyclic} \\ H \subseteq H^* \subseteq G}} \mu((H^* : H)), \tag{1}$$

where μ is the Möbius function.

THEOREM 1 (R. Brauer–S. Kuroda). *If F is a Galois extension of a number field k with the Galois group G, then*

$$\zeta_k(s) = \prod_{\substack{H \text{ cyclic} \\ H \subseteq G}} \zeta_{F^H}(s)^{c_G(H)}, \tag{2}$$

where F^H is the subfield of F fixed by H.

We say that the group G is *exceptional* if $c_G(E) = 0$, where $E = \{1\}$ is the trivial subgroup of G. Thus G is exceptional iff $\zeta_F(s)$ does not appear in the Brauer–Kuroda relation (2).

3. Main results

THEOREM 2. *If $G = G_1 \times G_2$, where $(|G_1|, |G_2|) = 1$, then*

$$c_G(E) = c_{G_1}(E_1) \cdot c_{G_2}(E_2),$$

where E, E_1 and E_2 are the trivial subgroups of G, G_1 and G_2, respectively. Hence G is exceptional iff G_1 or G_2 is exceptional.

Proof. Let H be a cyclic subgroup of G generated by an element $g = (g_1, g_2)$, where $g_1 \in G_1$, $g_2 \in G_2$. Since the orders $|g_1|$ and $|g_2|$ of the elements g_1 and g_2 are relatively prime, we have $|g| = |g_1|\,|g_2|$.

It follows that there is a 1-1 correspondence between the set of cyclic subgroups $H = \langle g \rangle$ of G and the set of all pairs of cyclic subgroups $(H_1, H_2) = (\langle g_1 \rangle, \langle g_2 \rangle)$ of G_1 and G_2, respectively. Thus $|H| = |H_1| \cdot |H_2|$, hence

$$\mu(|H|) = \mu(|H_1|) \cdot \mu(|H_2|),$$

since $(|H_1|, |H_2|) = 1$. Consequently,

$$\begin{aligned} c_G(E) &= \frac{1}{|G|} \sum_{\substack{H \text{ cyclic} \\ H \subseteq G}} \mu(|H|) = \frac{1}{|G_1|\,|G_2|} \sum_{\substack{H_1 \text{ cyclic} \\ H_1 \subseteq G_1}} \sum_{\substack{H_2 \text{ cyclic} \\ H_2 \subseteq G_2}} \mu(|H_1|)\mu(|H_2|) \\ &= \frac{1}{|G_1|} \sum_{\substack{H_1 \text{ cyclic} \\ H_1 \subseteq G_1}} \mu(|H_1|) \cdot \frac{1}{|G_2|} \sum_{\substack{H_2 \text{ cyclic} \\ H_2 \subseteq G_2}} \mu(|H_2|) = c_{G_1}(E_1) c_{G_2}(E_2). \ \blacksquare \end{aligned}$$

THEOREM 3. *If for some prime number p in G there is a unique subgroup of order p and it is contained in the center of G, then G is exceptional.*

Proof. Let H be the unique cyclic subgroup of G of order p. By assumption, it is contained in the center of G. By the definition (1) of $c_G(E)$, it follows that it is sufficient to consider cyclic subgroups of G of squarefree orders.

If H_1 is a cyclic subgroup of G of a squarefree order m not divisible by p, then $H_2 := HH_1$ is a cyclic subgroup of G, since H is contained in the center of G, and the orders of H and of H_1 are relatively prime. The order of H_2 is pm.

Conversely, if H_2 is a cyclic subgroup of G of a squarefree order pm divisible by p, then $p \nmid m$. Hence H_2 contains a subgroup of order p, which is H, by uniqueness. Moreover, H_2 is a direct sum of H and a cyclic subgroup H_1 of order m.

Thus, we get a 1-1 correspondence between the cyclic subgroups H_1 of G of squarefree orders not divisible by p, and the cyclic subgroups H_2 of G of squarefree orders divisible by p.

Moreover,

$$\mu(|H_1|) + \mu(|H_2|) = \mu(m) + \mu(pm) = \mu(m) - \mu(m) = 0,$$

and this implies that $c_G(E) = 0$. Thus the group G is exceptional. ∎

Corollary 1. *If in G there is a unique element of order 2, then G is exceptional.*

Proof. Let $a \in G$ be the unique element of order 2. Then for every $g \in G$ the element gag^{-1} has order 2. Therefore, by uniqueness, we get $gag^{-1} = a$, i.e. $ga = ag$ for every $g \in G$. Thus a belongs to the center of G, and the claim follows from Theorem 3 with $p = 2$. ∎

Corollary 2. *If for some prime number p the Sylow p-subgroup G_p of G is cyclic and is a direct summand of G, then G is exceptional.*

Proof. From the assumption it follows that G_p is contained in the center of G and there is a unique subgroup of order p in G_p, hence in G. The claim follows from Theorem 3. ∎

In the class of all p-groups the converse to Theorem 3 holds.

Theorem 4. *If a p-group $G \neq E$ is exceptional, then there is a unique subgroup of order p in G and it is contained in the center of G.*

Proof. Let k be the number of distinct subgroups of G of order p. Obviously $k \geq 1$. Since $\mu(p^r) = 0$ for $r \geq 2$, from (1) we get

$$c_G(E) = \frac{1}{|G|}(\mu(1) + k\mu(p)) = \frac{1}{|G|}(1 - k).$$

Hence $c_G(E) = 0$ iff $k = 1$.

Since the center of a p-group is nontrivial, it contains a subgroup of order p. By the uniqueness of the subgroup of order p, the claim follows. ∎

THEOREM 5. *If a group G contains a unique subgroup of order p, then either its Sylow p-subgroup G_p is cyclic, or $p = 2$ and G_p is (generalized) quaternion.*

Proof. See Theorem 5.3.7 in [KS]. ∎

THEOREM 6. *A p-group G is exceptional iff either G is cyclic, or $p = 2$ and G is (generalized) quaternion.*

Proof. If G is exceptional, then the claim follows from Theorems 4 and 5. Conversely, if G is cyclic, or if $p = 2$ and G is (generalized) quaternion, then there is a unique subgroup of G of order p, and it is contained in the center of G. Then, by Theorem 3, G is exceptional. ∎

We can also determine all exceptional groups in the class of nilpotent groups.

THEOREM 7. *A nilpotent group G is exceptional iff either for some prime number p its Sylow p-subgroup is cyclic, or its Sylow 2-subgroup is (generalized) quaternion. In particular, an abelian group is exceptional iff some of its Sylow subgroups is cyclic.*

Proof. A nilpotent group is a direct sum of its Sylow subgroups. Hence, by Theorem 2, the group is exceptional iff one of its Sylow subgroups is exceptional. The first part of theorem follows from Theorem 6. The second part follows from the observation that every abelian group is nilpotent, and the (generalized) quaternion group is not abelian. ∎

4. Examples of exceptional groups. Now, applying Corollary 1, we give examples of nonnilpotent exceptional groups. They are even nonsolvable.

THEOREM 8. *Let $\mathbb{F}$ be a finite field of odd characteristic. Then the group $G = \mathrm{SL}(2, \mathbb{F})$ has a unique element of order 2. Hence it is exceptional.*

Proof. Let $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}(2, \mathbb{F})$ have order 2. Then $M \neq I$ and $M^2 = I$. Hence $M = M^{-1}$, i.e.

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}.$$

It follows that $b = c = 0$ and $d = a$, $a^2 = 1$. Consequently, $M = -I$ is the unique element of order 2 in G. ∎

It is known that the group $\mathrm{PSL}(2, \mathbb{F})$ is simple, provided $|\mathbb{F}| > 4$. Therefore the group $\mathrm{SL}(2, \mathbb{F})$ is nonsolvable in this case.

Applying Theorems 5 and 8, it is easy to prove the well known result on the Sylow 2-subgroup of $\mathrm{SL}(2,\mathbb{F})$ (see Theorem 8.3(ii) on p. 42 of [G]).

THEOREM 9. *If* $\operatorname{char}\mathbb{F} > 2$*, then the Sylow* 2*-subgroup of* $\mathrm{SL}(2,\mathbb{F})$ *is* (*generalized*) *quaternion.*

Proof. By Theorem 8, the group $\mathrm{SL}(2,\mathbb{F})$ has a unique element of order 2. Thus, by Theorem 5, it is sufficient to prove that the Sylow 2-subgroup of $\mathrm{SL}(2,\mathbb{F})$ is not cyclic. For this purpose it is sufficient to find in $\mathrm{SL}(2,\mathbb{F})$ three elements of order 4.

In every finite field the form $x^2+y^2+z^2$ has a nontrivial zero. Hence, there exist $a,b\in\mathbb{F}$ satisfying $a^2+b^2+1=0$.

The matrices

$$M_1=\begin{pmatrix}0&1\\-1&0\end{pmatrix},\qquad M_2=\begin{pmatrix}0&-1\\1&0\end{pmatrix},\qquad M_3=\begin{pmatrix}a&b\\b&-a\end{pmatrix}$$

belong to $\mathrm{SL}(2,\mathbb{F})$, are distinct (since char $\mathbb{F}$ is odd), and satisfy $M_j^2=-I$ for $j=1,2,3$. Therefore M_1,M_2,M_3 have order 4. ∎

Now we give a general method for constructing groups with a unique element of order 2. By Corollary 1, this gives examples of exceptional groups.

THOREM 10. *Assume that a group* H *has a unique element of order* 2*, and let a group* G *be an extension of a group* K *of odd order by the group* H*, i.e. let the following exact sequence hold:*

$$1\to H\to G\xrightarrow{\varphi} K\to 1. \tag{3}$$

Then in G *there is a unique element of order* 2*.*

Proof. If $g\in G$ has order 2, then its image $\varphi(g)$ in K is 1, since the order of K is odd. Hence $g\in\ker\varphi=H$, and in H there is a unique element of order 2. ∎

We can apply Theorem 10 in the following way to construct effectively examples of nonnilpotent exceptional groups.

If in the group $\operatorname{Aut}H$ of automorphisms of H there is an element $\lambda\neq 1$ of odd order, then we put $K:=\langle\lambda\rangle$ and we consider the natural action of K on H. Then the semidirect product G of H by K with respect to λ, given by (3), is not the direct product of H and K.

In particular, if in H there is an element $h\neq 1$ of odd order not belonging to the center of H, then as λ we can take the inner automorphism defined by h.

For example, in the group Q of quaternions there is an automorphism of order 3 cyclically permuting the elements i,j,k. In $\mathrm{SL}(2,\mathbb{F})$ there is an element $M=\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$ of order $p=\operatorname{char}\mathbb{F}$, and it does not belong to the center of $\mathrm{SL}(2,\mathbb{F})$. So the inner automorphism of $\mathrm{SL}(2,\mathbb{F})$ determined by M

has order p. Applying Theorem 10 to these examples, we get an exceptional group containing Q as a subgroup of index 3, and an exceptional group containing $\mathrm{SL}(2,\mathbb{F})$ as a subgroup of index p, respectively.

Now we give examples of solvable nonnilpotent exceptional groups which do not satisfy the assumptions of Theorem 3.

LEMMA 1. *Let $V=\mathbb{F}_p^n$, where p is a prime number and $n\geq 1$. Then for every divisor $q>1$ of p^n-1 there is a matrix A of order q in $\mathrm{GL}(n,\mathbb{F}_p)$ whose eigenvalues are all different from 1. Moreover, the same is true for all A^r, where $r=1,\ldots,q-1$.*

Proof. Let $\mathbb{F}_{p^n}=\mathbb{F}_p(\zeta)$, where ζ is a generator of the cyclic group $\mathbb{F}_{p^n}^*$ (of order p^n-1). Let $f(x)$ be the minimal polynomial of ζ over $\mathbb{F}_p$ and $B\in\mathrm{GL}(n,\mathbb{F}_p)$ its companion matrix, hence $f(x)=\det(Bx-I)$.

Then the order of B in $\mathrm{GL}(n,\mathbb{F}_p)$ is p^n-1. Hence $A:=B^{(p^n-1)/q}$ has order q. The eigenvalues of B, that is, the zeros of $f(x)$ are ζ^{p^i} for $i=0,1,\ldots,n-1$. Thus the eigenvalues of A^r are the $r\frac{p^n-1}{q}$th powers of the eigenvalues of B. None of these powers is 1, since the order p^n-1 of ζ does not divide $p^i r\frac{p^n-1}{q}$ when $r=1,\ldots,q-1$. ∎

Now define H as the semidirect product of $V=\mathbb{F}_p^n$ by the subgroup $\langle A\rangle$ of $\mathrm{GL}(n,\mathbb{F}_p)$ with respect to the natural action of this subgroup on V, that is, H consists of pairs (v,A^r), where $v\in V,\ r=0,1,\ldots,q-1$, and

$$(v,A^r)(v',A^s)=(v+A^rv',A^{r+s}).$$

LEMMA 2. *The order of each element in H equals p or divides q.*

Proof. The elements (v,I), where $v\in V$ and $v\neq 0$, have order p. We claim that all the remaining elements of H with the exception of the neutral one, that is, the pairs (v,A^r), where $v\in V$ and $r=1,\ldots,q-1$, has order dividing q, that is, satisfy $(v,A^r)^q=I$. We have

$$(v,A^r)^q=(v+A^rv+\cdots+A^{r(q-1)}v,A^{rq}).$$

Denote $X:=I+A^r+\cdots+A^{r(q-1)}$. Then $XA^r=X$, since $A^q=I$. It follows that $X(A^r-I)=0$. But $\det(A^r-I)\neq 0$, since, according to Lemma 1, all eigenvalues of A^r are different from 1. Thus the matrix A^r-I is invertible, hence $X=0$ and it follows that $(v,A^r)^q=(Xv,A^{rq})=(0,I)$, as claimed. ∎

THEOREM 11. *Let p be a prime number and let $q>1$ be a squarefree integer not divisible by p. Assume that in a group H of order pq there is no element of order pd with $d>1$. Then the group $G:=\mathbb{Z}/pq\times H$ is exceptional.*

Proof. Every element of G has order dividing pq, so the order is squarefree. Denote by $N(r)$ the number of cyclic subgroups of G of order r. We fix a divisor $d>1$ of q and compare the numbers $N(pd)$ and $N(d)$.

Every cyclic subgroup H_2 of G of order pd contains unique subgroups H_1 and H_0 of orders d and p, respectively. Moreover $H_2 = H_1 \times H_0$.

Conversely, let H_1 be a fixed cyclic subgroup of G of order d. We look for subgroups H_0 of G of order p such that the group $\langle H_1, H_0\rangle$ is cyclic of order pd. This holds iff generators of H_1 and H_0 commute.

Let $h_1 := (u, v) \in \mathbb{Z}/pq \times H = G$ be a generator of H_1. Here $u \in \mathbb{Z}/pq$ and $v \in H$.

If $v \neq 1$, then the order d_1 of v satisfies $1 < d_1 \mid d$. It follows that h_1 does not commute with any element of order p in H, since, by assumption, in H there is no element of order pd_1. Obviously h_1 commutes with every element of order p in $\mathbb{Z}/pq$. Consequently, as H_0 we can take the unique subgroup of order p in $\mathbb{Z}/pq$.

If $v = 1$, then h_1 belongs to the center of G, so it commutes with every element of order p in G. Therefore as H_0 we can take any of the $N(p)$ subgroups of order p in G.

Thus we have proved that all but one of the $N(d)$ cyclic subgroups of G of order d are contained in an exactly one cyclic subgroup of G of order pd, and one cyclic subgroup of order d is contained in $N(p)$ cyclic subgroups of G of order pd.

Consequently, $N(pd) = N(d) - 1 + N(p)$, i.e.

$$N(pd) - N(d) = N(p) - 1. \tag{4}$$

Now we are ready to prove that the group G is exceptional. By the definition of $c_G(E)$ and (4), we have

$$\begin{aligned} c_G(E) &= \frac{1}{|G|}\sum_{k|pq}\mu(k)N(k) = \sum_{d|q}(\mu(pd)N(pd) + \mu(d)N(d)) \\ &= -\frac{1}{|G|}\sum_{d|q}\mu(d)(N(pd) - N(d)) = -\frac{N(p)-1}{|G|}\sum_{d|q}\mu(d) = 0, \end{aligned}$$

since $q > 1$. Thus the group G is exceptional. ∎

Corollary 3. *Let $p, q_1, \ldots, q_m$ be arbitrary different prime numbers. Then for $n = \varphi(q_1 \cdots q_m)$ there is an exceptional group of order $p^{n+r}q_1^{r_1+1}\cdots q_m^{r_m+1}$, where $r, r_1, \ldots, r_m$ are arbitrary positive integers, which is nonnilpotent and solvable.*

Proof. Since, by Euler's theorem, $q_1 \cdots q_m \mid p^{\varphi(q_1\cdots q_m)} - 1$, we may apply Lemma 2 and Theorem 11 with $q = q_1 \cdots q_m$ and $n = \varphi(q)$. We get the exceptional group $G = \mathbb{Z}/pq_1 \cdots q_m \times H$ of order $p^{n+1}q_1^2 \cdots q_m^2$.

The group

$$\widetilde{G} := \mathbb{Z}/p^r q_1^{r_1} \cdots q_m^{r_m} \times H$$

is also exceptional. Namely, by the definition of $c_{\widetilde{G}}(E)$, we have to consider

cyclic subgroups of $\widetilde{G}$ of squarefree orders only, therefore we can replace the group $\mathbb{Z}/p^r q_1^{r_1} \cdots q_m^{r_m}$ by its subgroup $\mathbb{Z}/pq_1 \cdots q_m$ and the value of $c_{\widetilde{G}(E)}$ will not change.

Obviously the group $\widetilde{G}$ is solvable and nonnilpotent. ∎

Acknowledgments. The authors thank the referee for valuable suggestions.

The first author thanks the third author for the hospitality during his visit at the Qingdao University, where the first version of this paper was written. The third author is supported by National Natural Science Foundation of China (No. 10871106).

References

[B] R. Brauer, *Beziehungen zwischen Klassenzahlen von Teilkörpern eines galoisschen Körpers*, Math. Nachr. 4 (1951), 158–174.

[G] D. Gorenstein, *Finite Groups*, Harper and Row, New York, 1968.

[K] S. Kuroda, *Über die Klassenzahlen algebraischer Zahlkörper*, Nagoya Math. J. 1 (1950), 1–10.

[KS] H. Kurzweil and B. Stellmacher, *The Theory of Finite Groups, An Introduction*, Springer, New York, 2004.

Jerzy Browkin
Institute of Mathematics
Polish Academy of Sciences
Śniadeckich 8
PL-00-956 Warszawa, Poland
E-mail: browkin@impan.pl

Juliusz Brzeziński
Mathematical Sciences
Chalmers University of Technology
and the University of Gothenburg
S-41296 Göteborg, Sweden
E-mail: jub@chalmers.se

Kejian Xu (corresponding author)
College of Mathematics
Qingdao University
Qingdao 266071, China
E-mail: kejianxu@amss.ac.cn

Received April 14, 2011;
received in final form July 25, 2011 (7826)