A Sylow-like theorem for integral group rings
of finite solvable groups

By

W. KIMMERLE and K. W. ROGENKAMP *)

1. Introduction. For a finite group \( G \) and a commutative ring \( R \) we denote by

\[
RG = \left\{ \sum_{g \in G} r_g \cdot g \right\}
\]

the group ring of \( G \) over \( R \). This group ring is an augmented algebra with

\[
\text{augmentation } \varepsilon: \ RG \to R, \ \sum_{g \in G} r_g \cdot g \to \sum_{g \in G} r_g.
\]

By \( V(RG) \) we denote the units in \( RG \), which have augmentation 1. The group of units in
\( RG \) is then the product of the units in \( R \) and \( V(RG) \).

A subgroup \( H \) of \( V(RG) \) with \(|H| = |G|\) is called a group basis, provided the elements
of \( H \) are linearly independent. This latter condition is automatic, provided no rational
prime divisor of \(|H|\) is a unit in \( R \) [1]. If \( H \) is a group basis, then \( RG = RH \) as augmented
algebras and conversely.

The object of this note is to prove the following

**Theorem 1.** Let \( G \) be a finite solvable group, and let \( H \) be a group basis of \( ZG \) with Sylow
\( p \)-subgroup \( P \). Then there exists a unit \( a \in QG \) such that \( aPa^{-1} \) is a Sylow \( p \)-subgroup of \( G \).

**Remark 1.** For solvable groups it was conjectured by Hans Zassenhaus [12, 11] that for any finite subgroup \( U \) of \( V(ZG) \) there exists \( a \in QG \) with \( aUa^{-1} \subseteq G \).

It is known that for a solvable group \( G \), the Sylow \( p \)-subgroups of different group bases
in \( ZG \) are isomorphic; however, the above result gives information about the embedding
of these Sylow \( p \)-subgroups into \( ZG \).

The isomorphism of the Sylow \( p \)-subgroups is an immediate consequence of the
following more general result: (\( \mathbb{Z}_p \) stands for the complete ring of \( p \)-adic integers.)

**Theorem 2 ([1]).** Let \( G \) be a finite group such that the generalized Fitting subgroup \( F^*(G) \)
is a \( p \)-group \(^{1} \). Then a group basis \( H \) of \( ZG \) is conjugate by a unit in \( Z_p G \) to a subgroup
of \( G \).

* The second author was partially supported by the DFG.

\(^{1}\) This is to say that \( G \) has a normal \( p \)-subgroup \( N \) with the centralizer \( C_G(N) \subseteq N \) or that the
generalized \( p' \)-core \( O_{p'}(G) \) is trivial [2, 3].
We shall state next a more general result, which does not only apply to solvable groups, and of which Theorem 1 is a special case – as will become transparent later on. For this we have to introduce some more notation.

**Definition 1.** Let $G$ be a finite group.

1. $\pi(G)$ is the set of rational prime divisors of $|G|$.
2. For the rational prime $p$, the group $O_p(G)$ is the largest normal subgroup of $G$ with order relatively prime to $p$.
3. $O_{p^r}(G)$ is the generalized $p^r$-core of $G$ [4, Ch. X, Paragraph 14].
4. Let $\pi$ be a finite set of rational primes. We call a finite group $G$ $\pi$-constrained, if for each $q \in \pi$ there exists a rational prime $p$ such that $O_{p^r}(G/O_{p^r}(G)) = 1$ and $q$ does not divide $|O_{p^r}(G)|$.

**Remark 2.** Note that in the above definition, the prime $q$ need not be different from $p$. Therefore a $p$-constrained group $G$ is also $\pi$-constrained for $\pi = \pi(G) \setminus \pi(O_{p^r}(G))$. Clearly a finite solvable group is $\pi$-constrained for every set of primes $\pi$. However, there are many insolvable groups which are $\pi$-constrained for some set $\pi$ (e.g. every Frobenius group is $\pi$-constrained for a suitable set $\pi$). It is not true though, that a $\pi$-constrained group $G$ is $p$-constrained for every $p \in \pi$ [2, 3].

We can now state the result, which we shall prove here:

**Theorem 3.** Let $G$ be a finite $\pi$-constrained group, and let $H$ be a group basis in $\mathbb{Z}G$. For each $p \in \pi$ and $P$ a Sylow $p$-subgroup of $H$, there exists a unit $a \in \mathbb{Q}G$ with $aPa^{-1}$ a Sylow $p$-subgroup of $G$.

2. **Connection with the Zassenhaus conjecture.** Let us return to a weak form of the Zassenhaus conjecture (cf. Remark 1):

**Conjecture 1** (Zassenhaus [12, 11]). Let $G$ be a finite group. If $H$ is a group basis in $\mathbb{Z}G$, then $H$ is conjugate in $\mathbb{Q}G$ to $G$; i.e. there exists a unit $a \in \mathbb{Q}G$ such that $aHa^{-1} = G$.

**Remark 3.** It was shown in [7] that the above conjecture is true for finite nilpotent groups. However, in [8] a metabelian group was constructed, which is a counterexample to the above Zassenhaus conjecture.

It is convenient, to rephrase the Zassenhaus conjecture in terms of *isomorphisms over class sums*.

**Definition 2.** Let $G$ be a finite group.

1. A class sum in $\mathbb{Z}G$ is an element of the form

$$CS_G(g) = \sum_{x \in G/C_G(g)} x^g;$$

i.e. the sum of the different conjugate elements of $g$.

2. Let $H$ be a group basis in $\mathbb{Z}G$. Then there is a class sum correspondence [1]: For every $h \in H$ there exists an element $\gamma(h) \in G$, such that $CS_H(h) = CS_G(\gamma(h))$ in $\mathbb{Z}G$. Note that $\gamma(h)$ is only determined up to conjugacy. Since the conjugacy class of $h$ and $\gamma(h)$ must have
the same cardinality – use the augmentation – the map \( \gamma \) can be extended to a
bijection \( \gamma: G \to H. \)

We shall call such a map a \textit{class sum correspondence}. Note that \( \gamma \) is in general not unique
and is in general not a homomorphism of groups; however, it sends \( p \)-power elements of
\( G \) to \( p \)-power elements of \( H \); it even preserves the order of the elements [6].

3. This class sum correspondence induces a correspondence between the normal subgroups of \( G \) and \( H \), essentially since a normal subgroup is a union of conjugacy classes, cf. e.g. [10].

4. Let \( H \) be a group basis in \( \mathbb{Z}G \). An isomorphism \( \varphi: H \to G \) is called an \textit{isomorphism
over the class sums} provided the induced automorphism – note \( \mathbb{Z}G = \mathbb{Z}H \) – which we
shall also denote by \( \varphi \)

\[
\varphi: \mathbb{Z}H \to \mathbb{Z}G, \quad \sum_{k \in H} r_k \cdot h \to \sum_{k \in H} r_k \cdot \varphi(h)
\]

has the property \( \varphi(CS_H(h)) = CS_G(\varphi(h)) \).

We can now reformulate the Zassenhaus conjecture – using the theorem of Skolem-Noether:

\textbf{Proposition 1.} The Zassenhaus conjecture is equivalent to the statement that for each
group basis \( H \) of \( \mathbb{Z}G \) there exists an isomorphism

\( \varphi: H \to G \)

– this means that the isomorphism problem has a positive answer – which is an isomorphism
over the class sums; with other words the above bijection

\( \gamma: H \to G \)

can be chosen to be a group isomorphism.

\textbf{Remark 4.} We shall collect here some observations:

1. Theorem 2 thus states, that in case \( F^*(G) \) is a \( p \)-group, then for every group basis \( H \) there exists an isomorphism over the class sums.

2. In our Theorems 1, 3 we are not dealing with the group basis, but rather with a
subgroup of a group basis \( H \). Thus we are looking for an extension of Proposition 1 to
a subgroup \( U \) of the group basis \( H \) (cf. Remark 1).

3. The obvious extension would be to require that the bijection \( \gamma \) in the Definition 2,2
could be chosen in such a way that it is a group isomorphism when restricted to \( U \).

\textbf{Theorem 4.} Let \( G \) be a finite group and let \( U \) be a finite subgroup of \( V(\mathbb{C}G) \). Denote by
\( L \) an algebraic number field such that \( U \subset LG \). Then the following statements are equivalent.

1. There exists a unit \( a \in LG \) with \( aUa^{-1} \subset G \).

2. There exists a group basis \( H \) of \( \mathbb{C}G \), and there exists a bijection

\( \varphi: H \to G \),
such that
\[ q_U : U \rightarrow q(U) \]
is a class sum preserving group isomorphism; i.e.
\[ CS_H(u) = CS_G(q(u)) \]
for every \( u \in U \). Moreover,
\[ |CS_H(u)| = |CS_G(q(u))|, \]
here \( |CS_G(g)| = |G : C_G(g)| \) denotes the number of elements conjugate to \( g \).

3. The Proofs.

Proof of Theorem 4. (1) \( \Rightarrow \) (2): If we take \( H = a^{-1} Ga \), then the conjugation by \( a \) is the desired map \( q \).

(2) \( \Rightarrow \) (1): Let \( L \subset K \) be an algebraic number field, which is a splitting field for \( G \) and choose a simple Wedderburn component \( A \) of \( KG = KH \).

Via the projection onto \( A \) we obtain two representations of \( U \), denoted by \( \phi_U \) and \( \phi_{q(U)} \) resp., where \( \phi_U \) is the representation of \( U \subset H \) and \( \phi_{q(U)} \) is the representation of \( U \) induced from \( q \).

We shall show that the characters for \( U \) of \( \phi_U \) and \( \phi_{q(U)} \) coincide. In fact, by assumption \( CS_H(u) = CS_G(q(u)) \) and so we have for the trace of \( \phi_U \) and \( \phi_{q(U)} \) resp. with \( l = |CS_H(u)| = |CS_G(q(u))| \):
\[
\text{tr}_{\phi_U}(u) = l^{-1} \cdot (l \cdot \text{tr}_{\phi_U}(u)) = l^{-1} \cdot (\text{tr}_{\phi_U}(CS_H(u)) = l^{-1} \cdot (\text{tr}_{\phi_{q(U)}}(CS_G(q(u)) = \text{tr}_{\phi_{q(U)}}(q(u)).
\]

This holds for every \( u \in U \), and since the characters determine a representation up to isomorphism (conjugacy), we conclude, that \( \phi_U \) and \( \phi_{q(U)} \) are conjugate in \( A \). Since this can be done for every simple Wedderburn component of \( KG \), we conclude that there exists \( b \in KG \) such that \( bUb^{-1} = q(U) \).

It remains to show that this conjugation can already be achieved in \( LG \). We shall be using bimodules to reach this goal:

We consider \( M = LG \) as \( L(U \times G) \)-bimodule, by letting \( U \) act in its natural way on \( M \) from the left and \( G \) acts on the right by its natural action. \( eM \) has the same right action as \( M \), but the left action is twisted by \( q \):
\[ u \cdot q m = q(u) \cdot m \]

Since \( U \) and \( q(U) \) are conjugate in \( KG \), the bimodules
\[ K \otimes_L M \quad \text{and} \quad K \otimes_L eM \]
are isomorphic. Invoking the Noether-Deuring theorem, we conclude that the bimodules \( M \) and \( eM \) must be isomorphic. Let
\[ M \rightarrow eM \]
be an isomorphism of \(L(U \times G)\)-bimodules. We put \(a = \tau(1)\). Then \(a\) is a unit in \(LG\) and moreover,
\[
\phi(u) \cdot a = a \cdot u
\]
for every \(u \in U\). \(\quad \text{q.e.d.}\)

The proof of Theorem 3 will now follow from Theorem 4, if we can show

**Proposition 2.** Let \(G\) be a finite \(\pi\)-constrained group for \(\pi\) a finite set of rational primes. \(H\) is a group basis in \(\mathbb{Z}G\).

For \(q \in \pi\) there exists by Definition 1.4 a prime \(p\) such that
\[
O_{p'}(G/O_{p'}(G)) = 1.
\]
Let \(S\) be a Sylow \(q\)-subgroup of \(H\). Then there exists a class sum correspondence
\[
\phi: H \rightarrow G
\]
such that
\[
\phi_S: S \rightarrow \phi(S)
\]
is a group isomorphism.

**Proof.** Let
\[
\kappa: \mathbb{Z}G \rightarrow \mathbb{Z}G/O_{p'}(G)
\]
be the augmented ring homomorphism induced from reduction modulo \(O_{p'}(G)\).

Since \(G\) is \(\pi\)-constrained, \(q\) does not divide \(|O_{p'}(G)|\), and so \(\kappa_1S\) injects \(S\) into \(\mathbb{Z}G/O_{p'}(G)\).

By the choice of \(p\), we may apply Theorem 2, to conclude that the Zassenhaus conjecture holds for \(\mathbb{Z}G/O_{p'}(G)\), and so there exists a class sum correspondence in
\[
\mathbb{Z}(\kappa(G)) = \mathbb{Z}(\kappa(H)),
\]
inducing an isomorphism of groups
\[
\bar{\phi}: \kappa(H) \rightarrow \kappa(G).
\]

With the correspondence of normal subgroups (Definition 2,3) we conclude that
\[
\ker(\kappa_1H) = O_{p'}(H)
\]
and that
\[
|O_{p'}(H)| = |O_{p'}(G)|.
\]
Thus we can find a Sylow \(q\)-subgroup of \(G\), say, \(T\) such that
\[
\bar{\phi}_{\kappa(S)}: \kappa(S) \rightarrow \kappa(T)
\]
is a group isomorphism.

Summarizing, we have now constructed a group isomorphism
\[
\phi_S = \kappa^{-1}_T \circ \bar{\phi} \circ \kappa_1S
\]
from \(S\) to \(T\).

**Claim 1.** Let now
\[
\gamma: H \rightarrow G
\]
be a class sum correspondence (Definition 2,2). Then
\[
CS_G(\gamma(s)) = CS_G(s) \quad s \quad s.
\]
Proof of the claim. Because of the class sum correspondence $\gamma$, there exists for every $s \in S$ an element $t \in T$ such that

$$CS_H(s) = CS_G(t)$$

- note that $\gamma$ sends $q$-power elements to $q$-power elements (Definition 2.2).

On the other hand, $\tilde{\varrho}$ induces the class sum correspondence on $\mathbb{Z}G/O_{p'}(G)$, and so we must have

$$CS_{G/O_{p'}(G)}(\kappa(t)) = CS_{G/O_{p'}(G)}(\tilde{\varrho} \circ \kappa(s)).$$

Thus $t$ is conjugate in $G$ to a $q$-power element of the form $w \cdot \varrho(s)$ for some $w \in O_{p'}(G)$. Note that we still have freedom in choosing $t$ in its conjugacy class. Thus we can assume that $t$ is such that $\kappa(t) = \kappa(q(s))$. In $O_{p'}(G) \cdot T$ the element $w \cdot \varrho(s)$ is - by Sylow's theorem - conjugate by an element $w_1 \in O_{p'}(G)$ to an element $t_1 \in T$. But then $\kappa(t) = \kappa(t_1)$ and so we must have $t = t_1$, since $\kappa_{|T}$ is injective.

Consequently $\varrho(s)$ and $t$ are conjugate.

This proves the claim and also finishes the proof of Proposition 2, and hence completes the proof of Theorem 3 and consequently of Theorem 1.

References


Eingegangen am 5.4.1990

Anschrift der Autoren:
W. Kimmerle
K. Roggenkamp
Mathematisches Institut B
Universität Stuttgart
Pfaffenwaldring 57
DW-7000 Stuttgart 80