On the torsion units in integral group rings of dihedral 2-groups

Alexander Zimmermann
Universität Stuttgart, Math. Inst. B,
Pfaffenwaldring 57, D-70550 Stuttgart, Germany

A. Weiss proved in [16] that for a p-group G and a finite subgroup U of the units of augmentation 1 of the group ring $\hat{\mathbb{Z}}_pG$ over the p-adic integers there exists a group basis containing U. In [12] K. W. Roggenkamp and L. L. Scott proved that all group bases in $\hat{\mathbb{Z}}_pG$ are conjugate. We will be concerned with the analogous question in $\mathbb{Z}G$, the integral group ring of a p-group G: *Are finite subgroups of the units of augmentation 1 of $\mathbb{Z}G$ subgroups of group bases?*

I. Hughes and K. E. Pearson showed in [8] that in the group of units of augmentation 1 of the integral group ring of the dihedral group of order 6 there is an involution not being part of any group basis. This involution however is not even part of a group basis in the group ring over the 2-adic integers. Therefore, they measure a local phenomenon rather than a global one. Furthermore, the dihedral group of order 6 is not a p-group and A. Weiss' theorem is not available. We investigate this problem for dihedral groups of order a power of 2 such that A. Weiss' theorem can be applied.

To go into details: Let D_{2^n} be the dihedral group of order 2^{n+1}. We denote by $V(RG)$ the group of units of augmentation 1 in the group ring of the finite group G over the integral domain R. The augmentation is the map induced by the trivial representation. As announced in [18] we will show that in $\mathbb{Z}D_{2^n}$ the number of conjugacy classes of involutions in $V(\mathbb{Z}D_{2^n})$ is equal to

$$1 + 2 \cdot 2^{n-1} \cdot \prod_{k=1}^{n} h_{2^k}^+$$

where $h^+_{2^k}$ is the class number of the maximal real subfield of $\mathbb{Q}(\zeta_{2^k})$, ζ_{2^k} being a primitive 2^k-th root of unity over $\mathbb{Q}$. We will show that the number of conjugacy classes of involutions in $V(\mathbb{Z}D_{2^n})$ consisting of elements that are part of a group basis is

$$1 + 2 \cdot 2^{n-1}.$$

Therefore, for each involution x in $V(\mathbb{Z}D_{2^n})$ there is a group basis H such that $x \in H$ if and only if the class number of $\mathbb{Z}[\zeta_{2^k} + \zeta_{2^k}^{-1}]$ is equal to 1 for all $k \leq n$. H. Cohn conjectured that this always happens (cf. [1]). The problem is therefore reduced to a conjecture in number theory.

As proved by S. Endo, T. Miyata and K. Sekiguchi in [3] the number of conjugacy classes of group bases is equal to $2^{n-1} \cdot 2^{n-2}$. If we use this result — it will follow independently and shorter from our arguments — we are able to give *generators for the group of outer central automorphisms of* $\mathbb{Z}D_{2^n}$ in terms of conjugation with group ring elements. Here we call an automorphism of a ring central if its restriction to the center is the identity.

In the integral group ring of the semidihedral group of order 16 there exists an involution that is not part of any group basis as is shown by the author in [19]. At the end of this paper we will give a sketch of the proof of the analogous statement for the semidihedral groups of order 2^{n+1}, n being an integral number greater than 3.

Our method is an application of the theory of K. W. Roggenkamp and L. L. Scott as reported in [11]. This theory is explained in detail in [13], so we restrict ourselves to give only some of the ideas of the theory.

Let G be a finite p-group and let U be a subgroup of G. We assume that $\mathbb{Z}G$ satisfies the Eichler condition (cf. [2]) and that the centralizer of U in $\mathbb{Z}G$ is commutative. We have to examine monomorphisms of U in $V(\mathbb{Z}G)$ that are induced by conjugation with a unit x of $\mathbb{Q}G$. These give rise to $\mathbb{Z}(U \times G)$ bimodules where U operates as multiplication by xUx^{-1} on the left and G acts as multiplication on the right, the so called twisted bimodule by conjugation x (cf. [5]). The isomorphism classes of those modules which are free $\mathbb{Z}G$ modules of rank one at the right and that become trivial if they are tensored up to $\mathbb{Q}$ parametrize the embeddings modulo conjugation with a unit in $\mathbb{Z}G$. This is easily seen since the bimodule $x\mathbb{Z}G$ is isomorphic to $\mathbb{Z}G$ if and only if modulo elements of the centralizer of U in $\mathbb{Q}G$ the element x is a unit of $\mathbb{Z}G$. Each of those embeddings can be realized by conjugation in $\hat{\mathbb{Z}}_qG$ for all primes q by the result of A. Weiss [16]. Similar

calculations as in the proof of A. Fröhlich's localization sequence (cf. [5]) give us an element of the class group of $C_{\mathbb{Z}G}(U)$ for each embedding modulo inner automorphisms of $\mathbb{Z}G$. This element of the class group lies in the kernel $Cl_{\mathbb{Z}G}(C_{\mathbb{Z}G}(U))$ of the induction map to the class group of $\mathbb{Z}G$ by the above. Conversely, if an element of the class group maps to the neutral element of the class group of $\mathbb{Z}G$ then it gives us a bimodule inducing an embedding. An element of $Cl_{\mathbb{Z}G}(C_{\mathbb{Z}G}(U))$ is in the image of the induction map from the class group of the center of $\mathbb{Z}G$ to the class group of the centralizer of U in $\mathbb{Z}G$ if and only if the corresponding conjugacy class of subgroups rationally conjugate to U consists of elements that are part of group bases. This is most easily seen by the fact that one obtains the bimodule for $\mathbb{Z}(U \times G)$ from the bimodule for $\mathbb{Z}(G \times G)$ by restricting the operation of G at the left to the subgroup U. This, however, corresponds to forming the induced module since also for Fröhlich's localization sequence one gets the $\mathbb{Z}(G \times G)$ bimodule from the ideal of the class group by inducing it to $\mathbb{Z}G$. Then the tensor product is associative and everything is done.

The major tool in calculating the class groups is Reiner-Ullom's version of Milnor's Mayer-Vietoris-sequence. For this purpose we write the various orders as pullbacks corresponding to the Wedderburn decomposition of $\mathbb{Z}D_{2^n}$. Afterwards we calculate the images of the global unit groups in several quotients to obtain the order of the class groups inductively. The group structure and the homomorphisms among the class groups are obtained by idèle theoretic arguments. The automorphism group of $\mathbb{Z}D_{2^n}$ is then easily obtained in a very explicit way by the previous results.

Acknowledgment: I want to express my thanks towards my academical teacher Professor Dr. K. W. Roggenkamp not only for his patient help but also for his encouragement and steady interest towards the progress of my thesis.

1. Preparations

We have to calculate some class groups and use several pullback diagrams for this topic. In general, a central idempotent e in the $\mathbb{Q}$-algebra A induces

a pullback diagram for the $\mathbb{Z}$-order Λ as follows:

$$\begin{array}{ccc} \Lambda & \longrightarrow & \Lambda \cdot e \\ \downarrow & & \downarrow \\ \Lambda \cdot (1-e) & \longrightarrow & (\Lambda \cdot e)\,/(\Lambda \cap (\Lambda \cdot e)) \end{array}$$

Since $e \in \mathbb{Q}\Lambda$, we can form $\Lambda \cdot e \subset \mathbb{Q}\Lambda$ and intersect it with $\Lambda \subset \mathbb{Q}\Lambda$. The intersection is a twosided ideal of $\Lambda \cdot e$. The quotient is denoted by $(\Lambda \cdot e)\,/(\Lambda \cap (\Lambda \cdot e))$. For $D_{2^n} :=< a, b \,|\, a^{2^n}, b^2, baba >$ we let

$$e_{n-1}^n := \frac{1}{2}(1 + a^{2^{n-1}})$$

and if we define

$$\begin{aligned} C(n) &:= C_{\mathbb{Z}D_{2^n}}(b) := \{x \in \mathbb{Z}D_{2^n} | xb = bx\} \\ &= < 1, b, a^i + a^{-i}, b(a^i + a^{-i}), a^{2^{n-1}}, a^{2^{n-1}}b | i = 1, ..., 2^{n-1} - 1 >_{\mathbb{Z}} \end{aligned}$$

we get pullback diagrams for $C(n)$, $\mathbb{Z}D_{2^n}$ and $B(n-1) := C(n) \cdot e_{n-1}^n$. Since

$$\mathbb{Z}D_{2^n} \cdot e \simeq \mathbb{Z}D_{2^{n-1}}$$

we may identify $B(n-1)$ with a subring of $\mathbb{Z}D_{2^{n-1}}$:

$$B(n-1) =< 1, b, a^i + a^{-i}, b(a^i + a^{-i}), 2a^{2^{n-1}}, 2a^{2^{n-1}}b | i = 1, ..., 2^{n-2} - 1 >_{\mathbb{Z}} .$$

Throughout the whole paper we abbreviate $\omega_n^+ := \zeta_{2^n} + \zeta_{2^n}^{-1}$ and $\omega_n^+(i) := \zeta_{2^n}^i + \zeta_{2^n}^{-i}$.

Since $\mathbb{Z}D_{2^n} \cdot (1 - e_{n-1}^n)$ is a suborder of the 2×2 matix ring over $\mathbb{Z}[\omega_n^+]$ (cf. [10]), we may identify $C(n) \cdot (1 - e_{n-1}^n)$ with $\mathbb{Z}[\omega_n^+] < b > \simeq \mathbb{Z}[\omega_n^+]C_2$ while denoting the cyclic group of order m by C_m. We observe that

$$B(n) \cdot (1 - e_{n-1}^n) = C(n) \cdot (1 - e_{n-1}^n)$$

with the above identification. We see that

$$C(n) \cdot (1 - e_{n-1}^n) \cap C(n) = 2\mathbb{Z}[\omega_n^+] < b >$$

and the quotient $\mathbb{Z}[\omega_n^+] < b > /(2\mathbb{Z}[\omega_n^+] < b >)$ is denoted by $\overline{B}(n-1)$. Analogously,

$$B(n) \cdot (1 - e_{n-1}^n) \cap B(n) = 2\omega_n^+\mathbb{Z}[\omega_n^+] < b >$$

and the quotient $\mathbb{Z}[\omega_n^+] < b > /(2\omega_n^+\mathbb{Z}[\omega_n^+] < b >)$ is denoted by $\tilde{B}(n-1)$. Furthermore, we observe that $B(n) \cdot e_{n-1}^n \simeq B(n-1)$.

We have now written the above defined orders $B(n)$ and $C(n)$ as pullbacks over smaller orders. It is now possible to apply Mayer-Vietoris sequences for the determination of the class groups of those orders.

2. Calculating the class number

We now give an upper bound for the class number of $C(n)$. This will be done by discussing the index of the image of the unit group of $\mathbb{Z}[\omega_n^+] < b >$ in $\overline{B}(n-1)$ and $\tilde{B}(n-1)$.

In [7] Gustafson and Roggenkamp gave generators for the image of the unit group of $Z[\omega_n^+]$ modulo 2.

Proposition 1 *Let π_2 be the natural epimorphism obtained by factoring the ideal of $\mathbb{Z}[\omega_n^+] < b >$ generated by 2 and let $\pi_{2\omega_n^+}$ be the natural epimorphism obtained by factoring the ideal generated by $2\omega_n^+$. Then*

1. $\pi_2(U(\mathbb{Z}[\omega_n^+] < b >)) = U(\overline{B}(n-1))$
2. $|U(\tilde{B}(n-1)) : \pi_{2\omega_n^+}(U(\mathbb{Z}[\omega_n^+] < b >))| = 2$.
   $2 - b$ *is not an element of* $\pi_{2\omega_n^+}(U(\mathbb{Z}[\omega_n^+] < b >))$.

Before proving Proposition 1 we establish two little lemmas:

Lemma 1 *$1 + \omega_n^+(i)$ and $b + \omega_n^+(i)$ are units in $\mathbb{Z}[\omega_n^+] < b >$ for all $i = 1, ..., 2^{n-1} - 1$.*

Proof: The elements in the first series are Galois conjugates of cyclotomic units of $\mathbb{Z}[\omega_n^+]$ and the second series can be mapped to elements of the first by the fact that

$$(b + \omega_n^+(i)) \cdot (b - \omega_n^+(i)) = -(1 + \omega_n^+(2i)).$$

Lemma 2 *Let $n \geq 2$ and $k \geq 2$ be natural numbers. If $(1+2^k x) \in U(\mathbb{Z}[\omega_n^+])$ for an $x \in \mathbb{Z}[\omega_n^+]$ then $x \in \omega_n^+\mathbb{Z}[\omega_n^+]$.*

Proof: We use induction over n. For $n = 2$ the statement is clear.

The field extension $\mathbb{Q}[\omega_n^+] : \mathbb{Q}[\omega_{n-1}^+]$ is quadratic. Let

$$x = \alpha + \sum_i \alpha_i \cdot \omega_n^+(2i) + \sum_j \beta_j \cdot \omega_n^+(2j+1) \in \mathbb{Z}[\omega_n^+]$$

be a generic element with integral coefficients. Then the nontrivial element σ of the Galois group of $\mathbb{Q}[\omega_n^+] : \mathbb{Q}[\omega_{n-1}^+]$ acts on x as

$$x^\sigma = \alpha + \sum_i \alpha_i \cdot \omega_n^+(2i) - \sum_j \beta_j \cdot \omega_n^+(2j+1) \in \mathbb{Z}[\omega_n^+]$$

and the norm nr down to $\mathbb{Q}[\omega_{n-1}^+]$ of $1 + 2^k x$ calculates as

$$\begin{aligned} nr(1+2^k x) &= 1 + 2^k tr(x) + 2^{2k} nr(x) \\ &= 1 + 2^{k+1}(\alpha + \sum_i \alpha_i \cdot \omega_n^+(2i) + 2^{k-1} nr(x)) \\ &\in U(\mathbb{Z}[\omega_{n-1}^+]) = U(\mathbb{Z}[\omega_n^+(2)]) \end{aligned}$$

tr being the trace. By induction we have

$$\alpha + \sum_i \alpha_i \cdot \omega_n^+(2i) + 2^{k-1} nr(x) \in \omega_n^+(2)\mathbb{Z}[\omega_n^+(2)],$$

If $n = 3$ all summands following α are even integers. The sum has to be even, and therefore, α is even, proving the assertion. If $n \geq 4$ then, since 2 and $\omega_n^+(2i)$ are multiples of $\omega_n^+(2)$, we conclude that $\alpha \in \omega_n^+ \mathbb{Z}[\omega_n^+]$. This proves the lemma.

Now we are able to prove that $2 - b \in U(\tilde{B}(n-1))$ is not an image of a unit of $\mathbb{Z}[\omega_n^+] < b >$ modulo $2\omega_n^+$.

The preimage of $2 - b$ is

$$2 - b + 2\omega_n^+ \mathbb{Z}[\omega_n^+] < b > .$$

This is in the Wedderburn components of the rational group algebra equal to

$$P_{2-b} := \{(1 + 2\omega_n^+(x+y), 3 + 2\omega_n^+(x-y)) | x, y \in \mathbb{Z}[\omega_n^+]\}.$$

Let

$$\varepsilon : \mathbb{Z}[\omega_n^+] < b > \longrightarrow \mathbb{Z}[\omega_n^+]$$

and

$$\overline{\varepsilon} : \tilde{B}(n-1) \longrightarrow \tilde{B}(n-1)/(b-1)\tilde{B}(n-1)$$

be the usual augmentation maps. Now $\overline{\varepsilon}(2-b) = 1$ and ε together with $\overline{\varepsilon}$ fit in a commutative square with respect to the projections modulo $2\omega_n^+$. Of course ε as well as $\overline{\varepsilon}$ are split by $x \longrightarrow x \cdot 1$. Therefore, if $u \in P_{2-b}$ also $u \cdot \varepsilon(u)^{-1} \in P_{2-b}$ and $u \cdot \varepsilon(u)^{-1}$ has augmentation 1. Assuming this to be done then in the set P_{2-b} the element $x + y = 0$ and the second component turns out to be $3 + 4\omega_n^+ y$ with $y \in \mathbb{Z}[\omega_n^+]$. Since

$$3 + 4\omega_n^+ y = -1 + 4(1 + \omega_n^+ y)$$

we are in the situation of the lemma. In fact $1 + \omega_n^+ y$ cannot belong to the prime ideal above 2 as requested and u cannot be a unit.

Now we come to the proof of Proposition 1: If part 1 is proved part 2 also follows: In fact, $\pi_{2\omega_n^+}$ factors through π_2 by the natural projection

$$\pi_{2,2\omega_n^+} : \tilde{B}(n-1) \longrightarrow \overline{B}(n-1)$$

so that $\pi_{2,2\omega_n^+} \circ \pi_{2\omega_n^+} = \pi_2$. The kernel of $\pi_{2,2\omega_n^+}$ is equal to $\{1, 1+2b, -1, -1+2b\}$ and has order 4 and therefore, the group index above is either $1, 2$ or 4. But -1 is in the kernel of π_2 and not in the kernel of $\pi_{2\omega_n^+}$ and hence the index is at most 2. This index is not equal to 1 because $2-b$ is not an image of a unit.

Therefore, we turn to the proof of part 1: We define the ring X_n to be equal to $\overline{B}(n)/((b+1)\overline{B}(n))$ and then we have, fixing the natural splitting $X_n \longrightarrow \overline{B}(n)$ obtained by $x \longrightarrow x \cdot 1$ and identifying the image with X_n,

$$U(\overline{B}(n)) = U(X_n) + (1+b) \cdot X_n$$

by the nilpotence of $(1+b)X_n$. For each $x, y \in X_n$ we multiply:

$$(1 + (1+b)x) \cdot (1 + (1+b)y) = 1 + (1+b)(x+y).$$

We will prove that

$$\tilde{Y}_n := \{1,\ \omega_n^+(i) \cdot (1 + \omega_n^+(i))^{-1} | i = 1, ..., 2^{n-1} - 1\} \subset \overline{B}(n)$$

gives a $\mathbb{Z}/2\mathbb{Z}$ basis for X_n. This fact will then prove Proposition 1 since $\{1+(b+1)x|x \in \tilde{Y}_n\}$ consists of images of global units and since by Gustafson and Roggenkamp (cf. [7]) $U(X_n)$ is generated by global units.

Set $X := X_n/X_{n-1}$ and let Y_n be the subvector space generated by $\tilde{Y}_n$. Then let Y be the image of Y_n in X. X_n is a subring of the group ring of the cyclic group of order 2^n by the identification $\zeta_{2^n} \longrightarrow a$ with a being a fixed generating element of C_{2^n}. Therefore, X_n is a module over the automorphism group of C_{2^n}. This automorphism group is isomorphic to $C_2 \times C_{2^{n-2}}$. However, the first factor, it sends a to a^{-1}, acts trivially on X_n and therefore, X_n is an $\mathbb{F}_2 C_{2^{n-2}}$-module. The projection $X_n \longrightarrow X$ is split as module homomorphism and we want to show that $Y_n = X_n$. For this purpose we show that $Y = X$. Since only the elements in

$$\{\omega_n^+(i) \cdot (1+\omega_n^+(i))^{-1} | i = 1, ..., 2^{n-1}-1, i \text{ odd } \}$$

are nonzero in Y, we have by induction that the set $\tilde{Y}_n$ is linearly independent and therefore generates X_n as a vector space.

If $Y < X$ we have that $Y \leq rad_{\mathbb{F}_2 C_{2^{n-2}}} X$ is annihilated by $\sum_{\sigma \in C_{2^{n-2}}} \sigma = \Delta$. But

$$\omega_n^+ \cdot (1+\omega_n^+)^{-1} = (\omega_n^+) + (\omega_n^+)^3 + (\omega_n^+)^5 + ...$$

in X. The powers greater than 1 come in even number of summands in the natural basis of X and vanish if one multiplies by Δ. Therefore, multiplication by Δ yields $\Delta \cdot \omega_n^+$ in the result, which is obviously not equal to zero. Hence, $Y = X$ and by induction $Y_n = X_n$. This proves Proposition 1.

If we now use the Mayer-Vietoris-sequences for the above pullback diagrams the following estimates can be given for the class groups of $B(n)$ and $C(n)$.

$$Cl(C(n)) = Cl(B(n-1)) \oplus Cl(\mathbb{Z}[\omega_n^+]C_2)$$

and

$$|Cl(B(n))| \in \{\lambda \cdot |Cl(B(n-1)) \oplus Cl(\mathbb{Z}[\omega_n^+]C_2)| \ : \lambda \in \{1,2\}\}.$$

We observe that $C(n)$ and also $B(n)$ are subrings of $\mathbb{Z}(C_{2^n} \times C_2)$ since both rings are commutative. Therefore, $f := \frac{1}{2}(1+b)$ induces pullback diagrams as introduced above. For abbreviation we write:

$$\hat{C}(n) := C(n) \cdot f \simeq C(n) \cdot (1-f), \hat{B}(n) := B(n) \cdot f \simeq B(n) \cdot (1-f),$$

$$\hat{\overline{C}}(n) := C(n) \cdot f/((C(n) \cdot f) \cap C(n)) = \hat{C}(n)/2\hat{C}(n),$$
$$\hat{\overline{B}}(n) := B(n) \cdot f/((B(n) \cdot f) \cap B(n)) = \hat{B}(n)/2\hat{B}(n).$$

We also, as usual, identify $\hat{B}(n)$ and $\hat{C}(n)$ with suitably chosen subrings of $\mathbb{Z}C_{2^n}$.

We apply a result of M. J. Taylor [14, 7.(2.10)] and Mayer-Vietoris-sequences of the pullback diagrams for $\hat{B}(n)$ and $\hat{C}(n)$ induced by f to obtain $Cl(\hat{B}(n)) = Cl(\hat{C}(n))$. Since $C(n)$ resp. $\hat{C}(n)$ are overorders of $B(n)$ rsp. $\hat{B}(n)$ in $\mathbb{Q}C(n)$ rsp. $\mathbb{Q}\hat{C}(n)$, we have induced epimorphisms of class groups of the smaller order to the larger one. Therefore, we have the following commutative (since Mayer Vietoris sequences are functorial) diagram with exact rows:

$$\begin{array}{ccccccccc} U(\hat{C}(n)) & \xrightarrow{\pi_C} & U(\hat{\overline{C}}(n)) & \longrightarrow & Cl(C(n)) & \longrightarrow & (Cl(\hat{C}(n))^2 & \longrightarrow & 0 \\ & & \uparrow & & \uparrow \alpha & & \| & & \\ U(\hat{B}(n)) & \xrightarrow{\pi_B} & U(\hat{\overline{B}}(n)) & \longrightarrow & Cl(B(n)) & \longrightarrow & (Cl(\hat{B}(n))^2 & \longrightarrow & 0. \end{array}$$

By the above, α is surjective. We are interested in the kernel. This is isomorphic to the kernel of

$$U(\hat{\overline{B}}(n))/\pi_B(U(\hat{B}(n)) \longrightarrow U(\hat{\overline{C}}(n))/\pi_C(U(\hat{C}(n)).$$

We observe that

$$U(\hat{\overline{B}}(n)) = 1 + 2\mathbb{Z}/4\mathbb{Z}a^{2^{n-1}} + \sum_i \mathbb{Z}/2\mathbb{Z}(a^i + a^{-i})$$

and that

$$U(\hat{\overline{C}}(n)) = 1 + \sum_i \mathbb{Z}/2\mathbb{Z}(a^i + a^{-i}) \cup a^{2^{n-1}} + \sum_i \mathbb{Z}/2\mathbb{Z}(a^i + a^{-i}).$$

Since $a^{2^{n-1}}$ is a unit in $\hat{C}(n)$ the kernel of the epimorphism

$$\beta : U(\hat{\overline{B}}(n)) \longrightarrow\!\!\!\!\!\rightarrow U(\hat{\overline{C}}(n))/ < a^{2^{n-1}} >$$

is cyclic of order 2. The sum of the coefficient of 1 and that of $a^{2^{n-1}}$ is odd since a unit has to have odd augmentation. Therefore, we immediately obtain that $U(\hat{C}(n))/ < a^{2^{n-1}} >= U(\hat{B}(n))$. We now show

Lemma 3 *No unit of $\hat{B}(n)$ maps onto the generating element of* $\ker(\beta)$.

Proof: We even show that there is no unit of $\hat{B}(n)$ that maps modulo $2^l\hat{B}(n)$ onto $1+2^la^{2^{n-1}}$ for $l \geq 1$. The crucial point is that the ring automorphism of $\mathbb{Z}C_{2^n}$ induced by $\sigma : a \longrightarrow -a$ induces a ring automorphism of $\hat{B}(n)$. Note that σ is the Galois automorphism from Lemma 2.

We prove the above by induction. For $n = 2$ the statement is trivial. Let $x = 1 + 2^la^{2^{n-1}} + 2^ly \in U(\hat{B}(n))$ with $y \in \hat{B}(n)$. Since $y + \sigma(y) \in 2\hat{B}(n)$, $x \cdot \sigma(x) = 1 + 2^{l+1}a^{2^{n-1}} + 2^{l+1}z$ for a $z \in \hat{B}(n)$. But

$$H^0(< \sigma >, \hat{B}(n)) = \hat{B}(n-1) \subset \hat{B}(n)$$

and therefore, since $\sigma(x \cdot \sigma(x)) = x \cdot \sigma(x)$ the element $x \cdot \sigma(x)$ is a preimage of $1 + a^{2^{n-1}}$ modulo 2^{l+1}. By induction $x \cdot \sigma(x)$ cannot be a unit, however, it is a unit by construction. We reached a contradiction and the lemma is proven.

Now we see that

$$|Cl(B(n))| = 2|Cl(C(n))|$$

and therefore, $|Cl(C(n))| = 2^{n-1}\prod_{k\leq n}|Cl(\mathbb{Z}[\omega_k^+] < b >)|$. Since

$$\mathbb{Z}[\omega_k^+] < b > \cdot\frac{(1+b)}{2} \simeq \mathbb{Z}[\omega_k^+] \simeq \mathbb{Z}[\omega_k^+] < b > \cdot\frac{(1-b)}{2}$$

a result of Taylor ([14, 7.(2.10)]) implies that

$$|Cl(\mathbb{Z}[\omega_k^+] < b >)| = |(Cl(\mathbb{Z}[\omega_k^+]))|^2 =: (h_{2^k}^+)^2.$$

Therefore,

$$|Cl(C(n))| = 2^{n-1} \cdot \prod_{k\leq n}(h_{2^k}^+)^2.$$

The main achievement of the above section is the determination of the size of the class group of $C(n)$ as well as the knowledge of $2-b$ as generator of the non trivial coset in the Mayer-Vietoris sequence corresponding to $B(n)$.

3. Embedding involutions into the unit group

We are interested in $K_n := ker(Cl(C(n)) \longrightarrow Cl(\mathbb{Z}D_{2^n}))$, the kernel of the induction homomorphism.

By Fröhlich, Keating and Wilson (cf. [6]) we have the following isomorphism:

$$Cl(\mathbb{Z}D_{2^n}) = Cl(\mathbb{Z}D_{2^{n-1}}) \oplus Cl(\mathbb{Z}[\omega_n^+])_{2\times 2}.$$

Fröhlich proved in [4] that $Cl(\mathbb{Z}D_2) = 1$. Induction behaves well with taking summands and so the kernel K_n is equal to a direct sum $K_n' \oplus K_n''$ according to the summation above.

For the moment we define $R_n := \mathbb{Z}[\omega_n^+]$. The following diagram has exact rows and columns:

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \to & C_2 & \to & K_n' & \to & K_{n-1}' \oplus K_{n-1}'' & \to & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \to & C_2 & \to & Cl(B(n-1)) & \to & Cl(B(n-2)) \oplus Cl(R_{n-1} < b >) & \to & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \to & 0 & \to & Cl(\mathbb{Z}D_{2^{n-1}}) & \to & Cl(\mathbb{Z}D_{2^{n-2}}) \oplus Cl((R_{n-1})_{2\times 2}) & \to & 0
\end{array}$$

The surjectivity at the top row follows by the serpent lemma. Therefore, we essentially have to calculate K_n'' to get the order of K_n. For this we use the representation given by K. W. Roggenkamp in [10]:

$$a \longrightarrow \begin{pmatrix} -1 & -1 \\ 2+\omega_n^+ & 1+\omega_n^+ \end{pmatrix}, b \longrightarrow \begin{pmatrix} -1 & 0 \\ 2+\omega_n^+ & 1 \end{pmatrix}.$$

By [2, Exercise 53.1] we see that an element of $Cl(\mathbb{Z}[\omega_n^+] < b >)$ is mapped to an element of $Cl((\mathbb{Z}[\omega_n^+])_{2\times 2})$ according to the following rule: If we have a pair of ideals $(\mathcal{A}, \mathcal{B})$ in $Cl((\mathbb{Z}[\omega_n^+])^2)$, it is represented by the idèle $\prod_{\wp \in Spec(\mathbb{Z}[\omega_n^+])}(2\alpha_\wp, 2\beta_\wp)$, say, which is mapped to the idèle

$$(\gamma) := \prod_{\wp} \begin{pmatrix} 2\alpha_\wp & 0 \\ (2+\omega_n^+)(\beta_\wp - \alpha_\wp) & 2\beta_\wp \end{pmatrix}$$

of $(\mathbb{Z}[\omega_n^+])_{2\times 2}$. Since we may calculate the norm locally (cf. [9, (24.2)] in connection with [9, (8.5)]) and intersect the local results afterwards we see that the reduced norm of the induced ideal is isomorphic to $\mathcal{AB}$. Therefore, we have that $K_n'' \simeq Cl(\mathbb{Z}[\omega_n^+])$ via the codiagonal in the direct sum of two copies of the class group of $Cl(\mathbb{Z}[\omega_n^+])$. Using now a theorem of

H. Weber ([15, p. 244, Satz C]) *the* $2'$*-Hall subgroup of* K_n *is isomorphic to* $\prod_{k=1}^{n} Cl(\mathbb{Z}[\omega_k^+])$.

On the whole we have

$$|K_n| = 2^{n-1} \cdot \prod_{k=1}^{n} h_{2^k}^+.$$

This formula presents the main achievement of the above section.

4. Connections to group bases

As we already did in the introduction we use for a suborder Γ of $\mathbb{Z}D_{2^n}$ the notation

$$Cl_{\mathbb{Z}D_{2^n}}(\Gamma) := ker(Cl(\Gamma) \longrightarrow Cl(\mathbb{Z}D_{2^n}))$$

Remind that in the previous sections we used the notation

$$Cl_{\mathbb{Z}D_{2^n}}(C_{\mathbb{Z}D_{2^n}}(b)) = Cl_{\mathbb{Z}D_{2^n}}(C(n)) = K_n.$$

We calculate the kernel and the image of the natural homomorphism

$$Cl_{\mathbb{Z}D_{2^n}}(Z(\mathbb{Z}D_{2^n})) \longrightarrow Cl_{\mathbb{Z}D_{2^n}}(C_{\mathbb{Z}D_{2^n}}(b)).$$

By S. Endo, T. Miyata and K. Sekiguchi ([3]) the first group is isomorphic to the outer central automorphism group and is furthermore the 2-Sylow subgroup of $Cl(Z(\mathbb{Z}D_{2^n}))$ by Weber's theorem. Hence, we have to deal with the 2-Sylow subgroup of $Cl(Z(\mathbb{Z}D_{2^n}))$.

Let e_k^n be the central idempotent that maps $\mathbb{Z}D_{2^n}$ onto $\mathbb{Z}D_{2^k}$ induced by the epimorphism $D_{2^n} \longrightarrow D_{2^k}$. Then the idèle

$$(\alpha_k(n)) := (((1 - e_k^n) + e_k^n \cdot (1 + 2b)) \times \prod_{p \neq 2} 1)$$

defines an element of $Cl(C(n))$. For $k = 1$ and $k = 0$ the idèle $\alpha_k(n)$ is central and hence defines an ideal of $C(n)$ isomorphic to one induced by an ideal of $Z(\mathbb{Z}D_{2^n})$.

Lemma 4 *Let* J *and* J' *be ideals of* $B(n)$ *with* $e_k^n \cdot J \simeq e_k^n \cdot J'$ *in* $B(k)$. *Then there is an element* $u \in < (\alpha_{n-1}(n)), ..., (\alpha_k(n)) >$ *with corresponding ideal* $\mathcal{U}$ *such that* $J \cdot \mathcal{U} \simeq J'$ *as* $B(n)$*-modules.*

Proof: This is trivial for $k = n-1$ and if it is true for all $k \in \{n-1, ..., k_0+1\}$, then by [2, Exercise 53.1] and Proposition 1.2. it is also true for $k = k_0$ and the lemma is proven.

Lemma 5 *The 2-Sylow subgroup of $Cl(C_{\mathbb{Z}D_{2^n}}(b))$ is cyclic, it is generated by $(\alpha_0(n))$ and it lies in the image of $Cl(Z(\mathbb{Z}D_{2^n}))$ under the induction map.*

Proof: We show that $(\alpha_k(n))$ has order 2^{n-k} in $Cl(B(n))$. One calculates easily, using [2, Exercise 53.1], that $e^n_{k+2} \cdot (\alpha_k(n))^2$ is equivalent to $e^n_{k+2}(\alpha_{k+1}(n))$ in $Cl(B(k+2))$ and therefore has order 2^{n-k-1} by induction. The remark following the definition of $(\alpha_k(n))$ completes the proof of the lemma.

We reached now the goal of the present section, namely to determine the structure of the class group of $C_{\mathbb{Z}D_{2^n}}(b)$, the kernel of the homomorphism of that class group to the class group of $\mathbb{Z}D_{2^n}$ as well as the image of the natural homomorphism of the class group of the centre of the integral group ring in the class group of the centralizer of b in the integral group ring.

If we use that by [16] every involution in $V(\mathbb{Z}G)$ is 2-adically conjugate to either $a^{2^{n-1}}, b$ or to ab and those can be distingished in the commutative quotient $\mathbb{Z}D_2$ we may summarize the above results in

Theorem 1 *Let $D_{2^n} =< a, b | a^{2^n}, b^2, baba >$ be the dihedral group of order 2^{n+1}. Let $h^+_{2^k}$ be the class number of the maximal real subfield of the field of 2^k-th roots of unity. Then*

1. *$Cl(C_{\mathbb{Z}D_{2^n}}(b)) \simeq C_{2^{n-1}} \times \prod_{k=1}^{n} (Cl(\mathbb{Z}[\omega_k^+]))^2$,*
2. *$Cl_{\mathbb{Z}D_{2^n}}(C_{\mathbb{Z}D_{2^n}}(b)) \simeq C_{2^{n-1}} \times \prod_{k=1}^{n} Cl(\mathbb{Z}[\omega_k^+])$.*
3. *In $V(\mathbb{Z}D_{2^n})$ there are $2^{n-1} \cdot \prod_{k=1}^{n} h_{2^k}$ conjugacy classes of involutions that are rationally conjugate to b.*
4. *In $V(\mathbb{Z}D_{2^n})$ there are 2^{n-1} conjugacy classes of involutions that are rationally conjugate to b and that are part of group bases.*
5. *Every involution in $V(\mathbb{Z}D_{2^n})$ is part of a group basis if and only if $h^+_{2^k} = 1$ for every $k \leq n$.*

Remark **1** One of the crucial points in [3] is to prove that there are elements of order 2^{n-1} in $Cl(Z(\mathbb{Z}D_{2^n}))$, an immediate consequence of our theorem.

5. Application to the automorphism group

We may use our result to give an explicit description of the outer automorphism group as conjugations with given group ring elements.

We first note that if a unit u of $\mathbb{Q}D_{2^n}$ normalizes a maximal order Λ of $\mathbb{Q}D_{2^n}$ containing $\mathbb{Z}D_{2^n}$ and if furthermore u normalizes $\hat{\mathbb{Z}}_2 D_{2^n}$, then u normalizes $\mathbb{Z}D_{2^n}$. This follows by the fact that we have to show it only locally and there it is obvious.

$1 + b \cdot (a + a^{-1})$ is a unit in $\hat{\mathbb{Z}}_2 D_{2^n}$. It normalizes the maximal order

$$\Gamma_n := \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z} \times \prod_{k=2}^{n} (\mathbb{Z}[\omega_k^+])_{2\times 2}.$$

This is seen most easily if one looks at its representation in Γ_n as given above. A. Whitcomb showed in [17] that conjugation by the rational unit $u_2 = 1 + a + ba$ yields a non inner automorphism of $\mathbb{Z}D_4$.

This result combined with our main theorem implies

Theorem 2 *The automorphism group of $\mathbb{Z}D_{2^n}$ is generated by the inner automorphisms, conjugation by $u_n = 1 + a + ba$ and conjugation by $v_n = 1 + b \cdot (a + a^{-1})$.*

The proof of Theorem 2 will fill the rest of section 5. We assume that conjugation with v_n is inner. Then there is a unit v' of $\mathbb{Z}D_{2^n}$ such that $v'^{-1} \cdot v_n$ is contained in the center of $\mathbb{Z}D_{2^n}$ and is also a unit in $\mathbb{Q}D_{2^n}$. First we examine the case $n = 3$. Then in Γ_3 we have

$$v_3 = 3 \oplus -1 \oplus -1 \oplus 3 \oplus \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \oplus \begin{pmatrix} 1-\sqrt{2} & 0 \\ 2+\sqrt{2} & 1+\sqrt{2} \end{pmatrix}.$$

v_2 is central and therefore since the center of $\mathbb{Z}D_4$ contains only the units ± 1 and $\pm a^2$ (it is a subring of $\mathbb{Z}(C_4 \times C_2)$) we immediately see that no central element of $\mathbb{Z}D_8$ carries v_3 to a unit v'.

Similar arguments can also be applied to conclude that conjugation by u_2 is not inner.

Since $Outcent(\mathbb{Z}D_{2^n}) \simeq Cl_{\mathbb{Z}D_{2^n}}(Z(\mathbb{Z}D_{2^n}))$ we see by an application of Mayer-Vietoris sequences and the fact that induction to overorders in the

same algebra yields epimorphisms of the class groups that the natural map $\mathbb{Z}D_{2^n} \longrightarrow\!\!\!\!\!\rightarrow \mathbb{Z}D_{2^{n-1}}$ induces an epimorphism

$$Outcent(\mathbb{Z}D_{2^n}) \longrightarrow\!\!\!\!\!\rightarrow Outcent(\mathbb{Z}D_{2^{n-1}}).$$

Now S. Endo, T. Miyata and K. Sekiguchi show ([3]) that

$$Outcent(\mathbb{Z}D_{2^n}) \simeq C_{2^{n-1}} \times C_{2^{n-2}} =: < \alpha_n > \times < \beta_n > .$$

Theorem 1 tells us that we may assume that β_n centralizes b for all n.

This is the point where we use the theorem!

Under this assumption $(\alpha_n)^j$ does not map b to a conjugate for all $j = 1, ..., 2^{n-1} - 1$. Let β'_n be a preimage of β_{n-1} such that β'_n centralizes b. Since β_{n-1} has no square root, β'_n has also none. Therefore, β'_n is an odd power of β_n.

Let α'_n be a preimage of α_{n-1}. Since β_n is in the kernel of the epimorphism $Outcent(\mathbb{Z}D_{2^n}) \longrightarrow Outcent(\mathbb{Z}D_4)$, α_{n-1}, and hence also α'_n maps to α_2. Therefore, α'_n has order 2^{n-1}. This proves Theorem 2 since we may choose $\alpha_n(x) = u_n x u_n^{-1}$ and $\beta_n(x) = v_n x v_n^{-1}$ for all $x \in \mathbb{Z}D_{2^n}$.

6. The semidihedral groups

Let S_n be the semidihedral group of order 2^{n+1} with the presentation

$$S_n =< a, b | a^{2^n} = b^2 = 1, bab = a^{2^{n-1}-1} > .$$

Factoring its center S_n maps onto $D_{2^{n-1}}$ and if one chooses $e := (1 + a^{2^{n-1}})/2$ then $\mathbb{Z}S_n \cdot (1 - e)$ embeds into the 2×2 matrix ring over R_n, the ring of algebraic integers in the fixed field of $\mathbb{Q}[\zeta_n]$ under the Galois automorphism sending ζ to $-\zeta^{-1}$. We observe that $C_{\mathbb{Z}S_n}(b) \cdot e = B(n-1)$ and that $C_{\mathbb{Z}S_n}(b) \cdot (1 - e) = R_n < b >$. The quotient $(C_{\mathbb{Z}S_n}(b) \cdot e)/(C_{\mathbb{Z}S_n}(b) \cdot e \cap C_{\mathbb{Z}S_n}(b))$ is isomorphic to $R_n < b > /2R_n < b >$. Since $2\mathbb{Z}$ is totally ramified in $\mathbb{Z}[\zeta_n]$ and hence also in R_n and since every unit besides -1 in R_n is a real unit, we can prove that

$$1 \longrightarrow C_2 \longrightarrow Cl(R_n < b >) \longrightarrow (Cl(R_n))^2 \longrightarrow 1$$

is exact. Let $\overline{\mathcal{A}}$ be the nontrivial ideal in the kernel. Then we shall show that there is an ideal of $C_{\mathbb{Z}S_n}(b)$ that, firstly, maps multiplied by e to an

ideal isomorphic to $B(n-1)$, secondly, maps multiplied by $1-e$ to an ideal isomorphic to $\overline{\mathcal{A}}$. This yields an ideal that, thirdly, maps, induced to an element of $Cl(\mathbb{Z}S_n)$, to the identity in $Cl(\mathbb{Z}S_n)$ and, fourth, that is not induced by an ideal of $Z(\mathbb{Z}S_n)$. Let $\mathcal{A}$ be an arbitrary ideal satisfying the first two conditions. The techniques for the dihedral groups may be applied to prove that $\overline{\mathcal{A}}$ maps to a principal ideal of the 2×2 matrix ring over R_n. Now $\overline{\mathcal{A}}$ is not induced by an ideal of $Z(\mathbb{Z}S_n)\cdot(1-e)$ as is easily seen. Therefore, by a theorem of Endo as quoted in [14, 3. 2.5] $\mathcal{A}$ maps either to 1 or to a Swan module which itself is induced by an ideal of $Z(\mathbb{Z}S_n)$. Elementary diagram chasing gives us the ideal satisfying the last two conditions and hence proving

Theorem 3 *In the group of units of augmentation 1 of the integral group ring of the semidihedral group S_n of order 2^{n+1} greater than* 16 *there is an involution that is not contained in any group basis of $\mathbb{Z}S_n$.*

References

[1] *N.C. Ankeney, S. Chowla, H. Hasse,* On the class number of the maximal real subfield of a cyclotomic field; J. reine angew. Math. 217 (1965), 217–220.

[2] *C. W. Curtis, I. Reiner,* Methods of Representation Theory Vol. 1 & 2; J. Wiley and Sons, New York 1982 & 1987.

[3] *S. Endo, T. Miyata, K. Sekiguchi,* Picard Groups and Automorphism Groups of Metacyclic Groups, J. Algebra 77 (1982), 286–310.

[4] *A. Fröhlich,* On the classgroup of integral grouprings of finite abelian groups; Mathematika 16 (1969), 143–152.

[5] *A. Fröhlich,* The Picard group of noncommutative rings, in particular of orders; Transactions of the Amer. Math. Soc. 180 (1973), 1–45.

[6] *A. Fröhlich, M. E. Keating, S. M. J. Wilson,* The Class Group of Quaternion and Dihedral 2–Groups; Mathematika 21 (1974), 64–71.

[7] *W. Gustafson, K. W. Roggenkamp,* A Mayer Vietoris sequence for Picard groups, with applications to integral group rings of dihedral and quaternion groups, Ill. J. of Math. 32 (1988), 375–406.

[8] *I. Hughes, K. E. Pearson,* The group of units in the group ring $\mathbb{Z}S_3$; Can. Math. Bull. 15 (1972), 529–534.

[9] *I. Reiner,* Maximal Orders; Academic Press, London 1975.

[10] *K. W. Roggenkamp,* Automorphisms and isomorphisms of integral group rings of finite groups; in Groups – Korea 1983, Springer Lecture Notes in Math. 1098, 118–135, 1984.

[11] *K. W. Roggenkamp,* The isomorphism problem and related topics; Bayreuther Mathematische Schriften 33 (1989), 173–196.

[12] *K. W. Roggenkamp, L.L. Scott,* Isomorphisms of p-adic group rings; Ann. of Math. 126 (1987), 593–647.

[13] *K. W. Roggenkamp, M. J. Taylor,* Group Rings and Class Groups; Birkhäuser Verlag, Basel 1992.

[14] *M. J. Taylor,* Classgroups of Group Rings; Cambridge University Press, Cambridge 1984.

[15] *H. Weber,* Theorie der abelschen Zahlkörper; Acta Math. 8 (1886), 193–263.

[16] *A. Weiss,* Rigidity of p-adic p-torsion; Ann. of Math. 127 (1988), 317–332.

[17] *A. Whitcomb,* The group ring problem; Ph. D. thesis, Univ. of Chicago 1968.

[18] *A. Zimmermann,* Involutions in Integral Group Rings of Certain Dihedral Groups; Math. Reports of the Acad. of Sc. of Canada XIV no. 4 (1992), 48–50.

[19] *A. Zimmermann,* Conjugacy of Involutions in Integral Group Rings of Certain Dihedral and Semidihedral Groups; Sitzungsberichte der gemeinnützigen Akademie der Wissenschaften zu Erfurt, Mathematisch Naturwissenschaftliche Klasse, Band 4 (1993).

[20] *A. Zimmermann,* Endliche Untergruppen der Einheitengruppe ganzzahliger Gruppenringe, Dissertation, Universität Stuttgart 1992.