Torsion units in integral group rings, conjugacy classes globally versus locally

Alexander Zimmermann*

Abstract

We give a series of examples for a program initiated by A. Weiss [18] to classify conjugacy classes of torsion units of integral group rings by a notion of 'genus'. The goal is there to compute on one hand side the number of genera and on the other hand side to compute the size of the different genera. In the present paper we examine dihedral groups of prime index and show that under certain restrictions on the prime index there are precisely 4 different genera of finite subgroups of the group of units of augmentation 1. We furthermore give, without restriction on the prime index, those conjugacy classes of torsion units which consist of elements belonging to group bases.

1 Introduction

The structure of the torsion units of the integral group ring $\mathbb{Z}G$ of a finite group G attained quite some attention since the breakthrough of K. W. Roggenkamp and L. L. Scott in 1987 (cf. [13]) and A. Weiss in 1988 (cf. [17]). A group ring is furnished with the structure of an *augmentation map* induced by the trivial representation. Denoting by $\hat{\mathbb{Z}}_p$ the p-adic integers, Roggenkamp and Scott proved [13] that for a finite p-group G every finite subgroup U of the units of $\hat{\mathbb{Z}}_pG$ of augmentation 1 is conjugate in the units of $\hat{\mathbb{Z}}_pG$ to a subgroup of G as long as the order of G equals the order of U. One year later, A. Weiss proved in [17] that the condition that the order of G equals the order of U is not necessary. The restriction to units of augmentation 1 is not essential since the units of the coefficient domain are a direct factor of the whole unit group.

For non p-groups the situation is much more complicate.

We denote for any finite group G and any Dedekind domain R by $V(RG)$ the group of units of RG with augmentation 1. A. Weiss introduced in [18] the notation of a *genus* of a finite subgroup U of the group of units of $\mathbb{Z}G$ of augmentation 1. The genus of U is the set of all $V(\mathbb{Z}G)$–conjugacy classes of subgroups V of $V(\mathbb{Z}G)$ such that for all primes q the groups U and V are conjugate in $V(\hat{\mathbb{Z}}_qG)$. By Weiss' result [17] for $p-$groups G, the genera of finite subgroups of $V(\mathbb{Z}G)$ are parametrized by the G–conjugacy classes of subgroups of G. For non p–groups no example was carried out so far. Weiss' project initiated in [18] divides the problem of determining the conjugacy class structure of finite subgroups of $V(\mathbb{Z}G)$ into two parts.
1) Determine all genera.
2) Determine for each genus its size.

Another problem is the question if a finite subgroup of $V(\mathbb{Z}G)$ can be extended to a group basis. A *group basis* of $\mathbb{Z}G$ is a subgroup U of the group of units of augmentation 1 such that U forms an additive basis for $\mathbb{Z}G$.

It was an open problem if there is a non $p-$group G and a unit u of augmentation 1 in $\mathbb{Z}G$ such that the group generated by u lies in the same genus as a finite subgroup of G but u is not an element of any group basis.

*The author acknowledges financial support from the Deutsche Forschungsgemeinschaft
1991 AMS-subject classification: primarily 16U60 and 16S34, secondary 20C10 and 20C05

The aim of the present paper now is twofold. First we give examples for a full computation of the different genera for a series of groups G. Secondly we give a series of examples for a computation of the cardinality of the genus of an involution containing a subgroup of G and determine which conjugacy class belongs to a conjugacy class of a maximal finite subgroup of the group of units of augmentation 1 and which can be extended to a group basis, and if this is possible, then in how many essentially different ways.

- Let $D_p =< a, b | a^p, b^2, baba >$ be the dihedral group of order $2p$ for an odd prime number p. All of the involutions in D_p are conjugate.
- For an abelian group A we use the notation $A^{[2]} = \{a^2 | a \in A\}$ and $A_{[2]} = \{a \in A | a^2 = 0\}$.
- We denote by ζ_p a primitive p-th root of unity and $\omega_p := \zeta_p + \zeta_p^{-1}$.
- We use the usual notation $h_p^+ := |Cl(\mathbb{Z}[\omega(p)])|$ and $h_p^- \cdot h_p^+ := |Cl(\mathbb{Z}[\zeta_p])|$.

Theorem 1 *1. In $V(\mathbb{Z}D_p)$ there are precisely*

$$\sigma_p := \frac{|Cl(\mathbb{Z}[\omega(p)]C_2)|}{|Cl(\mathbb{Z}[\omega(p)])|}$$

conjugacy classes of involutions being conjugate to b in $\hat{\mathbb{Z}}_q D_p$ for every prime number q. In other words, the genus (cf. [18]) of b splits into σ_p conjugacy classes.

2. Out of the conjugacy classes of involutions in 1. there are exactly

$$\tau_p := |Cl(\mathbb{Z}[\omega(p)])_{[2]}|$$

classes consisting of elements for which there is a group basis they are a part of.

3. b is contained in exactly $(p-1)/2$ conjugacy classes of group bases.

4. There is a further genus of involutions in $V(\mathbb{Z}D_p)$ which has the cardinality $|Cl(\mathbb{Z}[\omega(p)])|$. If 2 generates a prime ideal in $\mathbb{Z}[\omega(p)]$ and if $(2^{\frac{p-1}{2}} - 1, p-1) = 1$, then these are the only two genera of involutions.

5. In $V(\mathbb{Z}D_p)$ there is only one genus of subgroups of order p. This genus has cardinality

$$\frac{|Cl(\mathbb{Z}[\zeta_p])|}{|Cl(\mathbb{Z}[\omega(p)])|} \cdot \frac{p-1}{2} .$$

In case 2 generates a prime ideal in $\mathbb{Z}[\omega(p)]$ and if $(2^{\frac{p-1}{2}} - 1, p-1) = 1$ we get the following picture of the conjugacy class structure of units of finite order in $V(\mathbb{Z}D_p)$.

	genera		
order of elements	2	2	p
cardinality of the genus	σ_p	h_p^+	$\frac{p-1}{2} \cdot h_p^-$
contained in group bases	τ_p	0	$\frac{p-1}{2}$
number of group bases containing fixed element	$\frac{p-1}{2}$	0	τ_p

Examples for primes where both conditions are fulfilled are

$$\begin{aligned} p \in \{&3, 5, 7, 11, 19, 23, 29, 47, 53, 59, 67, 71, 79, 83, 101, 103, 107, 131, 139, 149, \\ &163, 167, 173, 179, 191, 197, 199, 227, 239, 263, 269, 271, 293, 317\} \end{aligned}$$

If 2 does not generate a prime ideal in $\mathbb{Z}[\omega(p)]$ or if $(2^{\frac{p-1}{2}} - 1, p-1) \neq 1$ then there are in general more genera of involutions.

Corollary 1 *[1] If there is a prime number q such that $4q^2$ divides $p-1$ and $(p-1)/(4q^2)$ is a square, then $\sigma_p > \tau_p$.*

A large number of conjugacy classes of involutions can be obtained using the results of Cornell and Washington [4] and that of Seah, Washington and Williams [15] for $p = 11290018777$. Most of them consist of elements that do not belong to any group basis, though, again all are conjugate locally to a group element.

We used the MAPLE V computer program to see, using results of van der Linden [16] that for the dihedral group of order $2 \cdot 37$ we get $\sigma_p = 3$ and $\tau_p = 1$. If we replace the number 37 by 101 the same holds true if we assume the generalized Riemann hypothesis.

In Statement 4. and 5. of Theorem 1 we use the theorem of Bhandari and Luthar [2] in which the number of conjugacy classes of involutions and that of subgroups of order p in $V(\mathbb{Z}D_p)$ are computed. The methods of Bhandari and Luthar are very different from ours.

In [7] Hughes and Pearson gave an example of a unit u of order 2 in the integral group ring $\mathbb{Z}S_3$ of the symmetric group of order 6 that generates a maximal finite subgroup of the group of units of augmentation 1, however, every group basis of $\mathbb{Z}S_3$ is conjugate in the units of $\mathbb{Z}S_3$ to S_3. Therefore, the unit u cannot be conjugate to an element of S_3 being naturally embedded in $\mathbb{Z}S_3$. However, u is not even conjugate in $\hat{\mathbb{Z}}_2 S_3$ to a group element. In fact, its conjugacy class is contained in the genus described in part 4. of the theorem. Fröhlich, Reiner and Ullom proved (cf. [6]) that for $p > 3$ there are $(p-1)/2 \cdot |Cl(\mathbb{Z}[\omega(p)])_{[2]}|$ conjugacy classes of group bases in $V(\mathbb{Z}D_p)$. All of the group bases are conjugate to D_p in the units of $\hat{\mathbb{Z}}_q D_p$ for every prime q.

Acknowledgement. Most of this work was done while I was preparing my dissertation. I want to thank Klaus W. Roggenkamp for his patience, help and encouragement.

2 The method

We shall use a method developed by K. W. Roggenkamp in collaboration with L. L. Scott and presented by K. W. Roggenkamp in [11] and [14, Part I Chapter VII]. The main idea is to interpret the conjugacy classes of subgroups of units as isomorphism classes of bimodules.

Proposition 1 *(K.W.Roggenkamp and L.L.Scott [11] and [14, Part I Chapter VII])*
Let G be a finite group and let U be a finite subgroup of $V(\mathbb{Z}G)$. Assume that $C_{\mathbb{Z}G}(U) := \{x \in \mathbb{Z}G \mid \forall\, u \in U : xu = ux\}$ is abelian and assume that $\mathbb{Z}G$ satisfies the Eichler condition. Let $V(\mathbb{Z}G)$ be the group of units of $\mathbb{Z}G$ of augmentation 1.

- *The number of conjugacy classes of subgroups H of $V(\mathbb{Z}G)$, which are in $\hat{\mathbb{Z}}_q G$ for all primes q conjugate to U is* [1]

$$Cl_{\mathbb{Z}G}(C_{\mathbb{Z}G}(U)) := ker(Cl(C_{\mathbb{Z}G}(U)) \longrightarrow Cl(\mathbb{Z}G)).$$

- *If $U \leq G$, then among them*

$$im(Cl_{\mathbb{Z}G}(C_{\mathbb{Z}G}(G)) \longrightarrow Cl_{\mathbb{Z}G}(C_{\mathbb{Z}G}(U)))$$

parametrizes the conjugacy classes of subgroups contained in group bases in the same genus as G and

$$ker(Cl_{\mathbb{Z}G}(C_{\mathbb{Z}G}(G)) \longrightarrow Cl_{\mathbb{Z}G}(C_{\mathbb{Z}G}(U)))$$

parametrizes the conjugacy classes of group bases in the genus of G containing U.

[1] $Cl(A)$ is the locally free class group of the $\mathbb{Z}$–order A. If we have an inclusion of $\mathbb{Z}$–orders $A \subseteq B$ then we get a homomorphism $B \otimes_A - : Cl(A) \longrightarrow Cl(B)$

The goal is, therefore, to compute the locally free class groups of the centralizer of U in $\mathbb{Z}G$. The method used in this direction is Milnor's Mayer Vietoris sequence in the version of Reiner and Ullom [10]. This sequence gives the class group, in case of presence of the Eichler condition and a pullback diagram of rings with epimorphic mappings, in terms of the class groups of the constituents and certain indices of unit groups. More precisely: Let R be a Dedekind domain with field of fractions K and let Λ be an R-order in the separable K-algebra A, satisfying the Eichler condition. Let, furthermore, $e^2 = e$ be a nontrivial idempotent in the centre of A. Then,

$$\begin{array}{ccc} \Lambda & \longrightarrow & \Lambda \cdot e \\ \downarrow & & \downarrow \varphi_+ \\ \Lambda \cdot (1-e) & \stackrel{\varphi_-}{\longrightarrow} & \Lambda \cdot e/(\Lambda \cdot e \cap \Lambda) \quad =: \quad \overline{\Lambda} \end{array}$$

is a pullback diagram with epimorphic mappings. We denote by $Cl(-)$ the locally free class group and by $U(-)$ the group of units. Then, Reiner and Ullom proved, that there is a mapping δ such that

$$1 \longrightarrow U(\overline{\Lambda})/ < \varphi_+(U(\Lambda \cdot e)) \cdot \varphi_-(U(\Lambda \cdot (1-e))) > \stackrel{\delta}{\longrightarrow}$$
$$\stackrel{\delta}{\longrightarrow} Cl(\Lambda) \longrightarrow Cl(\Lambda \cdot e) \times Cl(\Lambda \cdot (1-e)) \longrightarrow 1$$

is an exact sequence of abelian groups. We say that this pullback diagram and the Mayer Vietoris sequence are induced by the idempotent e.

3 The proof of the theorem

3.1 The principal genus of involutions

We shall prove in this section the first, the second and the third statement of Theorem 1. For this purpose we have to compute the relevant class groups via pullbacks and Mayer–Vietoris sequences.

We use the following notation:

- ζ_p is a primitive p^{th} root of unity.
- $\omega(p) := \zeta_p + \zeta_p^{-1}$ and $\omega_i(p) := \zeta_p^i + \zeta_p^{-i}$.
- $\mathbb{Z}[\omega(p)] = \mathbb{Z}[\zeta_p] \cap I\!R$ is the ring of algebraic integers of the maximal real subfield of the p^{th} cyclotomic field.
- $\pi := (1-\zeta_p) \cdot (1-\zeta_p^{-1})$ induces the unique prime above p in $\mathbb{Z}[\omega(p)]$.
- The prime field of characteristic p will be denoted by $I\!F_p$.

In $\mathbb{Q}D_p$ we have a central idempotent $e := \frac{1}{p}\sum_{i=1}^{p} a^i$. We shall look in the sequel at the pullback diagrams of $\mathbb{Z}D_p$, $C_{\mathbb{Z}D_p}(D_p)$ and $C_{\mathbb{Z}D_p}(b)$ associated to this idempotent.

Case $\mathbb{Z}D_p$: The pullback diagram associated to e is

$$\begin{array}{ccc} \mathbb{Z}D_p & \stackrel{\cdot e}{\longrightarrow} & \mathbb{Z} < b >= \mathbb{Z}C_2 \\ \downarrow \cdot(1-e) & & \downarrow \\ \begin{pmatrix} \mathbb{Z}[\omega(p)] & \mathbb{Z}[\omega(p)] \\ \pi \cdot \mathbb{Z}[\omega(p)] & \mathbb{Z}[\omega(p)] \end{pmatrix} & \longrightarrow & I\!F_p C_2 \end{array}$$

as is well known.

Case $C_{\mathbb{Z}D_p}(b)$**:** For the pullback assotiated to $C_{\mathbb{Z}D_p}(b)$ we see that since a goes to ζ_p in the two dimensional representation, the image of $C_{\mathbb{Z}D_p}(b)$ in Λ is $\mathbb{Z}[\omega(p)] < b >$. Moreover, $C_{\mathbb{Z}D_p}(b) \cdot e = \mathbb{Z}C_2$ and $C_{\mathbb{Z}D_p}(b)/(C_{\mathbb{Z}D_p}(b) \cap (C_{\mathbb{Z}D_p}(b) \cdot e)) = I\!F_pC_2$. The pullback diagram associated to e is now

$$\begin{array}{ccc} C_{\mathbb{Z}D_p}(b) & \stackrel{\cdot e}{\longrightarrow} & \mathbb{Z}C_2 \\ \downarrow \cdot(1-e) & & \downarrow \\ \mathbb{Z}[\omega(p)]C_2 & \longrightarrow & I\!F_pC_2 \end{array}$$

Case $C_{\mathbb{Z}D_p}(D_p)$**:** Though the computation of $Cl(Z(\mathbb{Z}D_p))$ is done in [5] and [6] by Fröhlich and Fröhlich, Reiner, Ullom we give the calculations within our terminology for the reader's convenience.

$$Z(\mathbb{Z}D_p) =< 1, a^i + a^{-i}, (1 + a + a^2 + ... + a^{p-1}) \cdot b | i = 1, ..., \frac{p-1}{2} > .$$

The pullback diagram for $Z(\mathbb{Z}D_p)$ corresponding to e is

$$\begin{array}{ccc} Z(\mathbb{Z}D_p) & \longrightarrow & \mathbb{Z} + p \cdot \mathbb{Z} \cdot b \\ \downarrow & & \downarrow \\ \mathbb{Z}[\omega(p)] & \longrightarrow & \mathbb{Z}/(p \cdot \mathbb{Z}). \end{array}$$

In the above three cases we use the Mayer Vietoris sequences and hence have to compute the images of the unit groups of the factors in their common finite quotient.

For this we use mainly two tools.
1) In $U(\mathbb{Z}[\omega(p)])$ there are units

$$u_k := 1 + \omega_1(p) + \omega_2(p) + ... + \omega_k(p) \text{ with } k = 1, ..., (p-3)/2$$

and

$$v_k := 1 - \omega_1(p) + \omega_2(p) - ... + (-1)^k \cdot \omega_k(p) \text{ with } k = 1, ..., (p-3)/2.$$

2) We use a theorem of Roggenkamp and Scott (cf. [12]): A unit in an order, which is a unit in an overorder in the same algebra, is a unit itself in the smaller order.

In the first case, Myrna Pike Lee [8] proved that each unit in the finite quotient is liftable to a unit to the two by two matrix ring. Hence,

$$Cl(\mathbb{Z}D_p) \stackrel{\cdot(1-e)}{\simeq} Cl(\mathbb{Z}[\omega(p)]).$$

In the third case, the units u_k and -1 for $k = 1, \ldots, (p-3)/2$ generate all of $U(\mathbb{Z}/(p \cdot \mathbb{Z}))$. The Mayer Vietoris sequence degenerates hence to

$$0 \longrightarrow Cl(C_{\mathbb{Z}D_p}(D_p)) \longrightarrow Cl(\mathbb{Z}[\omega(p)]) \oplus Cl(\mathbb{Z} + p \cdot \mathbb{Z}b) \longrightarrow 0$$

$Cl(\mathbb{Z} + p \cdot \mathbb{Z}b)$ is computed by the pullback diagram

$$\begin{array}{ccc} \mathbb{Z} + p \cdot \mathbb{Z} \cdot b & \longrightarrow & \mathbb{Z} \\ \downarrow & & \downarrow \\ \mathbb{Z} & \longrightarrow & \mathbb{Z}/(2 \cdot p \cdot \mathbb{Z}). \end{array}$$

corresponding to $f := (1 + b)/2$ as follows: The units in $\mathbb{Z}$ generate a subgroup of order 2 in the group of units in $I\!F_p$. Hence, this subgroup is cyclic of order $(p-1)/2$. The Mayer Vietoris sequence is then, using $Cl(\mathbb{Z}) = 1$,

$$1 \longrightarrow C_{\frac{p-1}{2}} \stackrel{\cdot f}{\longrightarrow} Cl(\mathbb{Z} + p \cdot \mathbb{Z} \cdot b) \longrightarrow 1.$$

Now,

$$Cl(Z(\mathbb{Z}D_p)) \simeq Cl(\mathbb{Z}[\omega(p)]) \oplus C_{\frac{p-1}{2}}.$$

In the second case, we proceed as follows. Define units

$$\alpha_k := \frac{1+b}{2}u_k + \frac{1-b}{2}v_k \in \mathbb{Z}[\omega(p)] < b > \text{ and } \beta_k := \frac{1-b}{2}u_k + \frac{1+b}{2}v_k \in \mathbb{Z}[\omega(p)] < b > .$$

Mapping b to 1, α_k maps to $2k+1$ and β_k to $(-1)^k$.
Mapping b to -1, β_k maps to $2k+1$ and α_k to $(-1)^k$.
But, $I\!F_p < b >= I\!F_p \oplus I\!F_p$ and we see that α_k and β_k for $k = 1, \ldots, (p-3)/2$ generate all the units in $I\!F_p C_2$.

The Mayer Vietoris sequence induced by e degenerates to

$$0 \longrightarrow Cl(C_{\mathbb{Z}D_p}(b)) \longrightarrow Cl(\mathbb{Z}[\omega(p)]C_2) \oplus Cl(\mathbb{Z}C_2) \longrightarrow 0.$$

Obviously, $Cl(\mathbb{Z}C_2) = 1$. We have to compute $Cl(\mathbb{Z}[\omega(p)]C_2)$. The idempotent $f := (1+b)/2$ induces a pullback diagram

$$\begin{array}{ccc} \mathbb{Z}[\omega(p)]C_2 & \longrightarrow & \mathbb{Z}[\omega(p)] \\ \downarrow & & \downarrow \\ \mathbb{Z}[\omega(p)] & \longrightarrow & \mathbb{Z}[\omega(p)] \otimes_{\mathbb{Z}} I\!F_2. \end{array}$$

The Mayer Vietoris sequence is at this point not generally exploitable since the structure of the unit groups is quite complicate and varies from prime to prime.

The next step which is needed to apply Proposition 1 is to compute the induction homomorphism of the class group of $C_{\mathbb{Z}D_p}(D_p) =: Z(\mathbb{Z}D_p)$ to that of $C_{\mathbb{Z}D_p}(b)$.

Denoting by λ the induction homomorphism we have the commutative diagram

$$\begin{array}{ccccccccc} & & & & 0 & & 0 & & \\ & & & & \uparrow & & \uparrow & & \\ 0 & \longrightarrow & & & \kappa'_p & \longrightarrow & \kappa'_p & \longrightarrow & 0 \\ & & & & \uparrow & & \uparrow & & \\ 0 & \longrightarrow & & & Cl(C_{\mathbb{Z}D_p}(b)) & \longrightarrow & Cl(\mathbb{Z}[\omega(p)]C_2) \oplus Cl(\mathbb{Z}C_2) & \longrightarrow & 0 \\ & & & & \uparrow & & \uparrow \lambda & & \\ 0 & \longrightarrow & & & Cl(Z(\mathbb{Z}D_p)) & \longrightarrow & Cl(\mathbb{Z}[\omega(p)]) \oplus Cl(\mathbb{Z} + p \cdot \mathbb{Z} \cdot b) & \longrightarrow & 0 \\ & & & & \uparrow & & \uparrow & & \\ 0 & \longrightarrow & & & \gamma_p & \longrightarrow & \gamma_p & \longrightarrow & 0 \\ & & & & \uparrow & & \uparrow & & \\ & & & & 0 & & 0 & & \end{array}$$

with exact rows and columns where γ_p and κ'_p are defined to be the kernel and the cokernel of γ respectively. Since $\lambda = \lambda \cdot (1-e) \oplus \lambda e$, and surely $\lambda \cdot (1-e)$ is injective,

$$|\kappa'_p| = \frac{|Cl(\mathbb{Z}[\omega(p)]C_2)|}{|Cl(\mathbb{Z}[\omega(p)])|} \text{ and } \gamma_p = C_{\frac{p-1}{2}}.$$

The next step which we need to apply Proposition 1 is to compute the kernels $Cl_{\mathbb{Z}D_p}(C_{\mathbb{Z}D_p}(D_p))$ of $Cl(C_{\mathbb{Z}D_p}(D_p)) \longrightarrow Cl(\mathbb{Z}D_p)$ and $Cl_{\mathbb{Z}D_p}(C_{\mathbb{Z}D_p}(b))$ of $Cl(C_{\mathbb{Z}D_p}(b)) \longrightarrow Cl(\mathbb{Z}D_p)$ as well as the image of $Cl_{\mathbb{Z}D_p}(C_{\mathbb{Z}D_p}(D_p)) \longrightarrow Cl_{\mathbb{Z}D_p}(C_{\mathbb{Z}D_p}(b))$.

The following commutative diagram with exact rows and columns is induced by the induc-

tion mapping to $\mathbb{Z}D_p$:

$$\begin{array}{ccccccccccc}
 & & & & 0 & & 0 & & 0 & & \\
 & & & & \uparrow & & \uparrow & & \uparrow & & \\
0 & \to & & & \kappa_p & \to & \kappa_p' & \to & \kappa_p'' & & \\
 & & & & \uparrow & & \uparrow & & \uparrow & & \\
0 & \to & Cl_{\mathbb{Z}C_p}(C_{\mathbb{Z}D_p}(b)) & \to & Cl(C_{\mathbb{Z}D_p}(b)) & \stackrel{\phi}{\to} & Cl(\mathbb{Z}[\omega(p)]) & & & & \\
 & & & & \uparrow & & \uparrow & & \uparrow & & \\
0 & \to & Cl_{\mathbb{Z}D_p}(Z(\mathbb{Z}D_p)) & \to & Cl(Z(\mathbb{Z}D_p)) & \stackrel{\psi}{\to} & Cl(\mathbb{Z}[\omega(p)])^{[2]} & \to & 0 & & \\
 & & & & \uparrow & & \uparrow & & \uparrow & & \\
0 & \to & \gamma_p & \to & \gamma_p & \to & 0 & & & & \\
 & & & & \uparrow & & \uparrow & & \uparrow & & \\
 & & & & 0 & & 0 & & 0 & &
\end{array}$$

Here, ϕ and ψ are just the induction homomorphisms to the maximal order

$$\begin{pmatrix} \mathbb{Z}[\omega(p)] & \mathbb{Z}[\omega(p)] \\ \mathbb{Z}[\omega(p)] & \mathbb{Z}[\omega(p)] \end{pmatrix} \oplus \mathbb{Z} \oplus \mathbb{Z}$$

in $\mathbb{Q}D_p$ containing $\mathbb{Z}D_p$. Lee [8] gives us the image of ψ. The injectivity of $\kappa_p \longrightarrow \kappa_p'$ follows from the serpent lemma. We obtain immediately:

$$ker[Cl_{\mathbb{Z}D_p}(Z(\mathbb{Z}D_p)) \longrightarrow Cl_{\mathbb{Z}C_p}(C_{\mathbb{Z}D_p}(b))] = \gamma_p = C_{\frac{p-1}{2}}.$$

The knowledge of γ_p leads to the knowledge of

$$|im(Cl_{\mathbb{Z}D_p}(Z(\mathbb{Z}D_p)) \longrightarrow Cl_{\mathbb{Z}D_p}(C_{\mathbb{Z}D_p}(b)))|.$$

Therefore, Statement 2. and 3. of Theorem 1 follows.

We now just have to compute the cokernel κ_p for determining $Cl_{\mathbb{Z}D_p}(C_{\mathbb{Z}D_p}(b))$ and by Proposition 1 the number of conjugacy classes in the genus of b. For this purpose we compute the image of ϕ.

To determine the image of ϕ we take an idèle $\alpha := (\alpha_\wp)_{\wp \in Spec\mathbb{Z}[\omega(p)]}$ of $\mathbb{Z}[\omega(p)]$ inducing the ideal $\mathcal{A}$, say. Then the idèle

$$\beta := \prod_{\wp \in Spec\mathbb{Z}[\omega(p)]} ((1+b) + (1-b) \cdot \alpha_\wp)$$

gives an ideal in Λ. Using the representation

$$a \longrightarrow \begin{pmatrix} 1 & 1 \\ \omega(p)-2 & \omega(p)-1 \end{pmatrix}, b \longrightarrow \begin{pmatrix} -1 & 0 \\ 2-\omega(p) & 1 \end{pmatrix}$$

we see that β is equal to

$$\beta = \prod_{\wp} \begin{pmatrix} 2\alpha_\wp & 0 \\ (2-\omega(p)) \cdot (1-\alpha_\wp) & 2 \end{pmatrix}$$

By [9, (24.2) & (8.5)] we can take the norms first and intersect afterwards, hence, β induces the ideal $4\mathcal{A} \simeq \mathcal{A}$. Therefore, ϕ is an epimorphism and so is $\kappa_p' \longrightarrow \kappa_p''$ by the serpent lemma.

We use the above commutative diagram to see that

$$\kappa_p'' = Cl(\mathbb{Z}[\omega(p)])/(Cl(\mathbb{Z}[\omega(p)])^{[2]}) \text{ and } |\kappa_p'| = \frac{|Cl(\mathbb{Z}[\omega(p)]C_2)|}{|Cl(\mathbb{Z}[\omega(p)])|}.$$

The size of κ_p can now be determined to

$$|coker[Cl_{\mathbb{Z}D_p}(Z(\mathbb{Z}D_p)) \longrightarrow Cl_{\mathbb{Z}D_p}(C_{\mathbb{Z}D_p}(b))]| = \\ = \frac{|Cl(\mathbb{Z}[\omega(p)]C_2|}{|Cl(\mathbb{Z}[\omega(p)])|^2} \cdot |Cl(\mathbb{Z}[\omega(p)])^{[2]}|.$$

This gives us Statement 1 in Theorem 1.

This gives us two sources for candidates for units not belonging to any group basis: Firstly, if h_p^+ is not a power of 2 and secondly if $|Cl(\mathbb{Z}[\omega(p)]C_2| \neq |Cl(\mathbb{Z}[\omega(p)])|^2$, the latter being the class number of a maximal order above $\mathbb{Z}[\omega(p)]C_2$.

By these discussions up to here the conjugacy class structure of the genus of b is completely determined.

3.2 The trivial genus of involutions

In this subsection [2] we shall prove Statement 4. of Theorem 1.

An involution v in another genus is given by the completely reducible representation $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$.

The centralizer in $\mathbb{Q}D_p$ of v is

$$\mathbb{Q}C := \begin{pmatrix} \mathbb{Q}[\omega(p)] & 0 \\ 0 & \mathbb{Q}[\omega(p)] \end{pmatrix} \times \mathbb{Q}C_2.$$

The centralizer of v in $\mathbb{Z}D_p$ is $C := \mathbb{Z}D_p \cap \mathbb{Q}C$. Clearly, $C \cdot (1-e) \simeq \mathbb{Z}[\omega(p)] \oplus \mathbb{Z}[\omega(p)]$. The units u_k from the beginning of Section 3.1 in both components generate $\overline{\Lambda} := (\mathbb{Z}/p \cdot \mathbb{Z})C_2$ modulo $\pi \cdot C \cdot e$.

Hence, the Mayer–Vietoris sequence corresponding to C with the idempotent e is

$$1 \longrightarrow Cl(C) \longrightarrow Cl(\begin{pmatrix} \mathbb{Z}[\omega(p)] & 0 \\ 0 & \mathbb{Z}[\omega(p)] \end{pmatrix}) \times Cl(\mathbb{Z}C_2) \longrightarrow 1.$$

But the kernel of the induction homomorphism to $Cl(\mathbb{Z}D_p) = Cl(\mathbb{Z}[\omega(p)])$ may then be calculated by the commutativity of the following diagram and the small observation following it:

$$\begin{array}{ccccccc} 1 & \longrightarrow & Cl(\mathbb{Z}D_p) & \longrightarrow & Cl(\mathbb{Z}[\omega(p)]) & \longrightarrow & 1 \\ & & \uparrow & & \uparrow \chi & & \\ 1 & \longrightarrow & Cl(C) & \longrightarrow & Cl(\mathbb{Z}[\omega(p)])^2 & \longrightarrow & 1 \end{array}$$

χ is an epimorphism since the ideal $\begin{pmatrix} \mathbb{Z}[\omega(p)] & 0 \\ 0 & \mathcal{A} \end{pmatrix}$ induced to the maximal order $(\mathbb{Z}[\omega(p)])_2$, the two by two matrix ring, is equal to $\mathcal{A}$ in the class group of $(\mathbb{Z}[\omega(p)])_2$.

Therefore, the kernel of $Cl(C) \longrightarrow Cl(\mathbb{Z}D_p)$ is equal to the kernel of χ, which has size equal to the order of $Cl(\mathbb{Z}[\omega(p)])$. In fact, it is isomorphic to $Cl(\mathbb{Z}[\omega(p)])$ via the codiagonal.

We now discuss cases where we have found all the conjugacy classes of involutions in the two genera discussed so far.

If we sum up the two cardinality of the two genera computed so far, we see that we have localized

$$n_p := (1 + \frac{|Cl(\mathbb{Z}[\omega(p)]C_2)|}{|Cl(\mathbb{Z}[\omega(p)])|^2}) \cdot h_p^+$$

conjugacy classes of involutions. Bhandari and Luthar (cf. [2]) get as a whole $\nu_0 \cdot h_p^+$ conjugacy classes of involutions where ν_0 is the number of equivalence classes of elements a in $\mathbb{Z}[\omega(p)]$, where two elements a and b are said to be equivalent if there is a unit u in $\mathbb{Z}[\omega(p)]$ with $u - 1 \in \pi\mathbb{Z}[\omega(p)]$ and $au - b \in 2\mathbb{Z}[\omega(p)]$.

[2] Most of the content of this subsection arose within a discussion with Klaus W. Roggenkamp

If 2 generates a prime ideal in $\mathbb{Z}[\omega(p)]$ then $\mathbb{Z}[\omega(p)]/(2\mathbb{Z}[\omega(p)])$ is a field and every non zero element in $\mathbb{Z}[\omega(p)] \setminus 2\mathbb{Z}[\omega(p)]$ maps to a unit.

Writing down the Mayer Vietoris sequence as done in the beginning for $\mathbb{Z}[\omega(p)]C_2$ for the idempotent f the index $|Cl(\mathbb{Z}[\omega(p)]C_2)|/|Cl(\mathbb{Z}[\omega(p)])|^2$ is just the number of congruence classes of units in $\mathbb{Z}[\omega(p)]/(2\mathbb{Z}[\omega(p)])$, where two elements a, b are to be called congruent, if a/b is the image of a unit in $\mathbb{Z}[\omega(p)]$. Hence, we have at least n_p/h_p^+ equivalence classes. However, being equivalent is a stronger relation as being congruent.

But, $2^{\frac{(p-1)}{2}} - 1$ is the size of $U(\mathbb{Z}[\omega(p)]/(2\mathbb{Z}[\omega(p)]))$ in case of 2 is prime, taking into account that 2 is unramified. Moreover, $p-1$ is the order of $U(\mathbb{Z}[\omega(p)]/(\pi\mathbb{Z}[\omega(p)]))$, since p is totally ramified.
We assume that the orders of these two unit groups of fields are coprime.
Given a and b two elements of $\mathbb{Z}[\omega(p)]$. If there is a $u \in U(\mathbb{Z}[\omega(p)])$, then this has order n in $\mathbb{Z}[\omega(p)]/(\pi\mathbb{Z}[\omega(p)])$, say, and order m in $\mathbb{Z}[\omega(p)]/(2\mathbb{Z}[\omega(p)])$, say. We get two integers α and β such that $\alpha n + \beta m = 1$. We see that $u^{1-\beta m} =: v$ has the property that $v - 1 \in \pi\mathbb{Z}[\omega(p)]$ since

$$v - 1 = (u^n)^\alpha - 1 \in \pi\mathbb{Z}[\omega(p)]$$

and

$$v \cdot a - b = u \cdot (u^m)^{-\beta} \cdot a - b = u \cdot a - b \in 2\mathbb{Z}[\omega(p)].$$

Hence, in this case being conguent is the same as being equivalent.

This proves that there is no further conjugacy class of involutions.

If 2 is not prime, then there are non zero elements in $\mathbb{Z}[\omega(p)]$ not being mapped to a unit modulo 2 and we get more genera of involutions. If the orders of the residue fields are not coprime then the condition of [2] that only units which become trivial modulo π operate, gives us more than two genera.

This proves Statement 4. of Theorem 1.

3.3 Units of odd order

In this section we shall prove Statement 5. of Theorem 1.

We have

$$D := C_{\mathbb{Z}D_p}(< a >) = \mathbb{Z} \cdot (1 + a + a^2 + ... + a^{p-1}) \cdot b + \sum_{i=1}^{p} \mathbb{Z} \cdot a^i.$$

Then

$$D \cdot e = \mathbb{Z} + p \cdot \mathbb{Z} \cdot b \text{ and } D \cdot (1 - e) = \mathbb{Z}[\zeta_p]$$

interpreting Λ as twisted group ring $\Lambda \simeq \mathbb{Z}[\zeta_p] \otimes_{\mathbb{Z}} \mathbb{Z}C_2$. Then, $D \cdot e/(D \cdot e \cap D) = \mathbb{Z}/(p \cdot \mathbb{Z})$. The units $u_k \in \mathbb{Z}[\zeta_p]$ generate again $\mathbb{Z}/(p \cdot \mathbb{Z})$ modulo $(1 - \zeta_p) \cdot \mathbb{Z}[\zeta_p]$. We get the Mayer Vietoris sequence

$$1 \longrightarrow Cl(D) \longrightarrow Cl(\mathbb{Z} + p\mathbb{Z}b) \times Cl(\mathbb{Z}[\zeta_p]) \longrightarrow 1.$$

The kernel of $Cl(D) \longrightarrow Cl(\mathbb{Z}D_p)$ is calculated componentwise if we use $Cl(\mathbb{Z}D_p) = 1 \times Cl(\mathbb{Z}[\omega(p)])$. The mapping splits as direct product of two mappings, according to the idempotent e and in the first component we have the kernel $C_{\frac{p-1}{2}}$. In the last component we observe that $Cl(\Lambda) \simeq Cl(\mathbb{Z}[\omega(p)])$ via the reduced norm map. This, however, coincides with the interpretation as twisted tensor product with the usual number theoretic norm. Then, the norm map is surjective on the class groups, as is well known.

Therefore, the number of conjugacy classes of subgroups of order p of $V(\mathbb{Z}D_p)$ that are locally conjugate to $< a >$ is equal to

$$\frac{p-1}{2} \cdot h^- := \frac{p-1}{2} \cdot \frac{|Cl(\mathbb{Z}[\zeta_p])|}{|Cl(\mathbb{Z}[\omega(p)])|}.$$

Coleman's result (cf. [3] and [14, Part I Chapter II § 2]) [3] tells us that in $V(\hat{\mathbb{Z}}_p D_p)$ a unit of order p is conjugate to a power of a if and only if it is conjugate in D_p already to a group element. Therefore, in $V(\hat{\mathbb{Z}}_p D_p)$, the genus of $< a >$ splits into $(p-1)/2$ conjugacy classes. Hence, using the result in Bhandari and Luthar [2], we see that for units of order p there is no other genus than the principal genus.

References

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

[2] *A. K. Bhandari and I. S. Luthar,* Conjugacy classes of torsion units of the integral group ring of D_p, Comm. in Alg. 11 (14) (1983), 1607–1627.

[3] *D. Coleman,* On the modular group ring of a p-group, Proc. Amer. Math. Soc. 15 (1964), 511–514.

[4] *G. Cornell and L. C. Washington,* Class Numbers of Cyclotomic Fields, J. Number Theory 21 (1985), 260–274.

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

[6] *A. Fröhlich, I. Reiner and S. Ullom,* Class groups and Picard groups of orders, Proc. London Math. Soc. (3) 29 (1974), 405–434.

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

[8] *M. P. Lee,* Integral representations of dihedral groups of order $2p$, Trans. of Amer. Math. Soc. 110 (1964), 213–231.

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

[10] *I. Reiner and S. Ullom,* A Mayer-Vietoris Sequence for Class Groups, J. Algebra 31 (1974), 305–342.

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

[12] *K. W. Roggenkamp and L. L. Scott,* Units in metabelian group rings: non-splitting examples for normalized units, J. of Pure and Appl. Alg. 27 (1983), 299-314.

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

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

[15] *E. Seah, L. C. Washington and H. Williams* The Calculation of a Large Cubic Class Number With an Application to Real Cyclotomic Fields, Math. Comp. 41 (1983), 303–305.

[16] *F. J. van der Linden,* Class Number Computations of Real Abelian Number Fields, Math. Comp. 39 no.160 (1982), 693–707.

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

[18] *A. Weiss,* Torsion units in integral group rings, J. reine angew. Math. 415 (1991), 175–187.

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

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

Address of the author: Mathematisches Institut B, Universität Stuttgart, D-70550 Stuttgart, Germany,
e-mail: Zimmermann@mathematik.uni-stuttgart.de

Current address: UFR de Mathématiques; Université de Paris 7; 2, place Jussieu; 75251 Paris Cedex 05; France.

[3] In fact, Roggenkamp and Scott generalized Coleman's result to the following: If P is a p-subgroup of the finite group G, then the normalizer of P in $V(\hat{\mathbb{Z}}_p G)$ equals the normalizer of P in G times the centralizer of P in $V(\hat{\mathbb{Z}}_p G)$.