On the Galois module structure of units in met acyclic extensions

McGaul, Karen Yvonne

On the Galois module structure of units in metacyclic extensions

by

Karen Yvonne McGaul

A thesis presented for

for the degree of Doctor of Philosophy

August 1996

Department of Mathematical Sciences,

University of Durham,

South Road, Durham,

DH1 3LE, England

Abstract.

On the Galois module structure of units
in metacyclic extensions - Karen Y. McGaul

Let Γ be a metacyclic group of order pq with p and q prime. We shall show that the Γ-cohomology and character of a Γ-lattice determine its genus.

Let N/L be a Galois extension with group Γ, then U_N, the torsion-free units of N, is a Γ-lattice and the isomorphism $\mathbb{Q} \otimes U_N \cong \mathbb{Q} \otimes \Delta S_\infty$ gives its character. In certain cases we can determine its cohomology and thus its genus; in particular, when $h_N = 1$ and $L = \mathbb{Q}$ we show that the genus of U_N depends only on the number of non-split, ramified primes in N/L.

We shall also investigate U_N in the factorizability defect Grothendieck group.

Preface.

On the Galois module structure of units
in metacyclic extensions - Karen Y. McGaul

I would firstly like to acknowledge my supervisor Steve Wilson for all his help, patience and encouragement. I would also like to thank my friends in the department who have made my time in Durham very enjoyable, in particular, my office mates Mansour Aghasi, Mike Gronow, Paul Jones, Helen Fawley, and Michael Young. Also, thanks to Ulrich Harder for his comments and suggestions on my thesis and for his encouragement. Last, but not least, I would like to thank my family for their support throughout my education.

This work has been sponsored by the U.K. Engineering and Physical Sciences Research Council.

The thesis is based on research carried out between October 1992 and May 1996. It has not been submitted for any other degree either at Durham or at any other University. The results in Chapters 3 to 8 are original work apart from the first section of each or where indicated otherwise.

Contents

CHAPTER 1

Introduction.

Let N and L be algebraic number fields and N a Galois extension of L with group Γ. Let $\mathcal{E}_N$ be the group of multiplicative units of the algebraic integers of N and μ_N its torsion subgroup. Then there exists a finitely-generated $\mathbb{Z}\Gamma$-lattice, U_N, defined by the exact sequence

$$0 \to \mu_N \hookrightarrow \mathcal{E}_N \to U_N \to 0.$$

U_N will be referred to as the torsion-free units of N. In this thesis we are particularly interested in the Galois module structure of U_N in the case when Γ is a non-abelian metacyclic group of order pq where p and q are prime.

Many results on the Galois module structure of units concentrate on determining whether or not U_N has a Minkowski unit (see [Du], [Ma2] for some non-cyclic examples and [Ma1], [Mo1], [Mo2] for specifically metacyclic examples or section 1.2). We will discuss the metacyclic case in section 1.2. There are also general results on local units (see [GW1], [GW2] for general results or [Ja2], [Ja3] for local metacyclic extensions) discussed in Chapter 3 and on S-units (see for example [GW1]) which we discuss in Chapter 4.

A finite group Γ has finite representation type if and only if all its p-Sylow subgroups have order 1, p or p^2 ([CR1], theorem 33.6). This means there is only a finite number of indecomposable Γ-lattices and it seems logical to describe U_N as a direct sum of these.

In general however, though there are still a finite number of indecomposable lattices of each $\mathbb{Z}$-rank, it would be difficult to describe the possible genera of U_N for a general extension N/L.

When Γ is abelian then there are many techniques available which make it possible to get more complete descriptions of the Galois module structure of U_N, or at least to say when U_N is in the same genus as a module of which the structure is known. We shall discuss the results of [Bu] and [Fr] on real abelian extensions in the next section.

When Γ is metacyclic of order pq with p and q prime then there are finitely many indecomposable Γ-lattices and an example of a lattice from each genus is given in section 1.2. Since $U_N \otimes \mathbb{Q} \cong \Delta S_\infty \otimes \mathbb{Q}$ we know the characters of U_N which gives finitely many possibilities for its genus.

This idea is used in the papers by Moser ([Mo1] and [Mo2]) to find invariants determining the genus of U_N. The invariants found are in terms of indices between unit groups (see section 1.2).

We shall show that the characters and cohomology of a Γ-lattice (where Γ is pq-metacyclic) determine its genus (theorem 2.6). This will enable us to find the genus of U_N (and other Γ-lattices) in certain cases. In particular, when h_N, the class number of N, is trivial and $L = \mathbb{Q}$ we find U_N is determined completely by the number of non-split, ramified primes in $N/\mathbb{Q}$ (theorem 6.6).

We shall also apply these results to local units and S-units. Finally, in Chapter 7 we shall use a different technique and show that working in the factorizability defect Grothendieck group can give some interesting results on the Galois structure of U_N.

1.1. Abelian extensions.

Here we recount the work of [Fr] and [Bu] on abelian extensions. For any abelian group Γ, let $T_\Gamma = \sum_{\gamma \in \Gamma} \gamma$ be the trace element of the integral group ring $\mathbb{Z}\Gamma$. Let A_Γ be the semi-simple $\mathbb{Q}$-algebra $\mathbb{Q}\Gamma/\mathbb{Q}T_\Gamma$. Then there is a $\mathbb{Z}$-order $\mathcal{A}_\Gamma$ of A_Γ defined by the exact sequence

$$0 \to \mathbb{Z}T_\Gamma \to \mathbb{Z}\Gamma \to \mathcal{A}_\Gamma \to 0.$$

Let L possess a unique infinite place, which is the same as L being either the field of rationals, $\mathbb{Q}$, or an imaginary quadratic field. If Γ is the Galois group of N/L then there is a natural action of $\mathcal{A}_\Gamma$ on U_N. Let $\mathcal{A}_N$ be the associated order of U_N in A_Γ, i.e. identifying U_N with $U_N \otimes \mathbb{Z} \subset U_N \otimes \mathbb{Q}$, $\mathcal{A}_N$ is the full set of elements of A_Γ which induce endomorphisms of U_N. Clearly $\mathcal{A}_\Gamma \subset \mathcal{A}_N$.

The problem studied in [Bu] is to determine the conditions under which U_N is locally free as an $\mathcal{A}_N$-lattice. Equivalently, when do U_N and $\mathcal{A}_N$ lie in the same $\mathcal{A}_\Gamma$-genus?

Before giving some answers to this question we need a few definitions.

Definitions. Let Γ^* be the group of complex multiplicative characters of Γ and let $\mathcal{P}(\Gamma^*)$ be the set of subgroups of Γ^*. For a subgroup Ω of Γ, $\mathcal{G}(\Omega) \in \mathcal{P}(\Gamma^*)$ is the set of characters which act trivially on Ω. Two characters of Γ belong to the same **division** if and only if the generate the same cyclic subgroup of Γ^*. Thus to a division D there corresponds a cyclic subgroup $\bar{D}$ of Γ^*.

Let $f \in \mathrm{Map}(\mathcal{P}(\Gamma^*), \mathbb{Q}_{>0})$ then f can be extended to each division D of Γ^* using the Möbius μ-function

$$f(D) = \prod_{C \leq \bar{D}} f(C)^{\mu(|\bar{D}|/|C|)},$$

and we get a rational number $\widetilde{f}$ from f called the **factor derivative** defined by

$$\widetilde{f} = (\prod_{D \subset \Gamma^*} f(D)) f(\Gamma^*)^{-1},$$

where the product is over all divisions D of Γ^*.

$$\widetilde{\mathcal{J}}_\Gamma = (\prod_p p^{J_p}) \frac{1}{|\Gamma|},$$

$$J_p = \text{no. of non-trivial divisions of } \Gamma_p^*,$$

Define $h_{N/L} \in \mathrm{Map}(\mathcal{P}(\Gamma^*), \mathbb{N})$ to be

$$h_{N/L} : \mathcal{G}(\Omega) \mapsto \mathrm{hcf}(h_{N^\Omega}, |\Gamma|).$$

where h_{N^Ω} is the class number of N^Ω.

Define the map $w_{N/L} \in \mathrm{Map}(\mathcal{P}(\Gamma^*), \mathbb{N})$ to be

$$w_{N/L} : \mathcal{G}(\Omega) \to \mathrm{hcf}(w_{N^\Omega}, |\Gamma|).$$

where w_{N^Ω} is the cardinality of the torsion units of N^Ω.

A subgroup Ω of Γ is **cocyclic** if Γ/Ω is cyclic, and write $\Omega <_c \Gamma$.

Theorem 1.1. *([Bu], theorem 3) Let L possess a unique infinite place (so L is either $\mathbb{Q}$ or an imaginary quadratic field). Let N/L be an abelian extension which is unramified at infinity. Then $U_N \vee \mathcal{A}_\Gamma$ if and only if both $\widetilde{h}_{N/L} = \widetilde{w}_{N/L}\widetilde{\mathcal{J}}_\Gamma$ and $H^0(\Omega, U_N) = 0$ for all cocyclic subgroups $\Omega <_c \Gamma$.* □

Note that H^0 means Tate cohomology.

More specifically, when $L = \mathbb{Q}$ and $[N : \mathbb{Q}]$ is a power of a prime we have

Theorem 1.2. *([Fr], theorem 5) Let N be a real abelian extension of $\mathbb{Q}$. Let $[N : \mathbb{Q}]$ be a power of a prime l. If*

(i) *Γ is cyclic, there is exactly one ramified prime and this prime ramifies totally,*
(ii) *there are exactly two primes which ramify in N and each is inert in its inertia field. Also l is odd,*

then U_N is a locally-free $\mathcal{A}_\Gamma$-module. □

In general it is difficult to calculate $\widetilde{h}_{N/L}$ and hence to find the structure of the units. However, for a prime l, when the Hilbert l-class field of N is abelian over L it is possible to find the local structure.

This is certainly true if N is contained in F which is an abelian l-extension of L and $l \nmid h_F$. F is then called a **genus field extension** of L.

Definitions. The place $v \in S_{F/L}$, the set of non-archimedean places of L which ramify in F/L, is associated to the prime $\mathcal{O}_L$ ideal $\mathcal{P}_v$. If $\mathcal{P}_v$ has order h_v in Cl_L then choose $\pi_v \in L$ such that

$$\mathcal{P}_v^{h_v} = \pi_v \mathcal{O}_L.$$

$I_{F/L,v}$ = inertia group of v in Gal(F/L).

$D_{F/L,v}$ = decomposition group of v in Gal(F/L).

If v is coprime to l, fix an element $x_v \in \mathcal{O}_v$, the valuation ring of L_v, which generates the multiplicative group of $R_v := \mathcal{O}_v/\mathcal{P}_v\mathcal{O}_v$, for each element $z \in \mathcal{O}_v^*$ define $[v,z] \in \mathbb{Z}_l/(\#R_v)\mathbb{Z}_l$ by

$$z \equiv x_v^{[v,z]} \mod \mathcal{P}_v\mathcal{O}_v.$$

If $v|l$ and $I_{F/L}$ is cyclic then choose a place w of F lying above v and fix a generator $x_v \in \mathcal{O}_v^*$ of the quotient group $\mathcal{O}_v^*/\mathrm{Norm}_{F_w/K_v}(\mathcal{O}_w^*)$. For $z \in \mathcal{O}_v^*$ define $[v,z] \in \mathbb{Z}_l/e_v\mathbb{Z}_l$ by

$$z \equiv x_v^{[v,z]} \mod \mathrm{Norm}_{F_w/K_v}(\mathcal{O}_w^*).$$

Theorem 1.3. *([Bu], theorem 6) Let F be a genus field extension of L of degree l^3 and $S_{F/L} = \{v_1, v_2, v_3\}$ such that*

$$\begin{pmatrix} -[v_2, \pi_{v_2}] & -[v_3, \pi_{v_1}] & 0 \\ [v_1, \pi_{v_2}] & 0 & -[v_3, \pi_{v_2}] \\ 0 & [v_1, \pi_{v_3}] & [v_2, \pi_{v_3}] \end{pmatrix} \in GL_3(\mathbb{F}_l).$$

If $C \leq$ Gal(F/L) is a subgroup of order l satisfying

(i) $C \cap I_{F/L,v_i} = 1$ *for each* $i = 1, 2, 3$,

(ii) $C \cap (\cap_{i=1}^{i=3} D_{F/L,v_i}) = 1$, *then with* $K = F^C$ *one has*

$$U_K \vee \mathcal{A}_K. \quad \square$$

1.2. Metacyclic extensions.

N is a Galois extension of L over $\mathbb{Q}$. Let $\Gamma = \mathrm{Gal(N/L)}$ be a metacyclic group of order pq.

$$\Gamma = \langle \sigma, \tau | \sigma^p = \tau^q = 1, \tau\sigma\tau^{-1} = \sigma^r \rangle$$

where p and q are distinct primes, p odd and $q|(p-1)$. The integer r is a primitive qth root of unity modulo p. When $q = 2$ then Γ is dihedral.

It is well known that Γ has finite representation type. There are $2^q + 2^{q-1} + q + 2$ genera of indecomposable $\mathbb{Z}\Gamma$-lattices, but a general lattice need not decompose uniquely into a product of indecomposable lattices. These results come from Pu, [Pu] and in the dihedral case, originally in Lee, [Le].

Listed below is an example of a lattice from each genus, using the notation of [CR1].

Lattice	Description	No. of genera	Character
(i) P_i, $(0 \le i \le q-1)$	$P = (1-\xi_p)\mathbb{Z}[\xi_p]$ where σ acts as mult. by ξ_p, and τ acts as the automorphism $\xi_p \mapsto \xi_p{}^r$. $P_i = P^i$ and $P_0 = R = \mathbb{Z}[\xi_p]$.	q	χ
(ii) $\mathbb{Z}$	σ and τ act trivially.	1	χ^+
(iii) $\mathbb{S} = \mathbb{Z}[\xi_q]$	σ acts trivially, τ acts as mult. by ξ_q.	1	χ^-
(iv) $\mathbb{Z}[C_q]$	σ acts trivially,	1	$\chi^+ + \chi^-$

τ acts as mult. by τ.

(v) X_T	The non-split extension $0 \to L_T \to X_T \to \mathbb{S} \to 0,$	$2^{q-1} - 1$	$\lvert T\rvert\chi + \chi^-$
(vi) Y_T	The non-split extension $0 \to L_T \to Y_T \to \mathbb{Z}[\mathcal{C}_q] \to 0.$	$2^q - 1$	$\lvert T\rvert\chi + \chi^+ + \chi^-$
(vii) V	The non-split extension $0 \to P \to V \to \mathbb{Z} \to 0.$	1	$\chi + \chi^+$

where T is a non-empty subset of $\{0, 1, \ldots, q-1\}, L_T = \amalg_{t \in T} P_t$. (excluding in the X_T case $t = 1$, which must split.) $\mathrm{char}(\mathbb{Z}\Gamma) = \chi^+ + \chi^- + q\chi$ and for a rational prime r, ξ_r is a primitive rth root of unity.

χ^+ is the trivial character, $\chi^- = \chi_1^- + \cdots + \chi_{q-1}^-$ is the sum of irreducible characters of dimension 1 corresponding to the conjugacy classes of σ^i, and $\chi = \chi_1 + \cdots + \chi_{(p-1/q)}$ is the sum of characters of dimension q.

Remark $Y_{T^{\max}}$ where $T^{\max} = \{0, 1, \ldots, q-1\}$ is in the same genus as $\mathbb{Z}\Gamma$.

In the dihedral case we shall use a slightly different notation, again from [CR1]. Let Γ be a dihedral group of order $2p$. Then there are 10 indecomposable Γ-lattices; $\mathbb{Z}$ where Γ acts trivially, $\mathbb{Z}^-$ where τ acts as multiplication by -1 and σ acts trivially, $\mathbb{Z}\mathcal{C}_2$ where σ acts trivially, $R = \mathbb{Z}[\xi_p], P = (1 - \xi_p)R$ where σ acts as multiplication by ξ_p and τ as complex conjugation, V, X, Y_0, Y_1, Y_2 are respectively the non-split extensions of $\mathbb{Z}$ by P, $\mathbb{Z}$ by R, $\mathbb{Z}\mathcal{C}_q$ by R, $\mathbb{Z}\mathcal{C}_q$ by P, and $\mathbb{Z}\mathcal{C}_q$ by $R \oplus P$.

Let $N/\mathbb{Q}$ be a real, metacyclic extension of order pq with p and q odd primes, q divides $p - 1$. Let $\mathcal{C}_p = \langle\sigma\rangle$ and $\mathcal{C}_q = \langle\tau\rangle$. Let $K = N^{\mathcal{C}_p}$ and $k = N^{\mathcal{C}_q}$.

Let Γ be the Galois group of $N/\mathbb{Q}$ and let $\chi^*_{\{1\}}$ be the character of Γ induced from the trivial character of $\{1\}$ and χ_Γ is the trivial character of Γ. Then the character of U_N is $\chi^*_{\{1\}} - \chi_\Gamma$. From section 1.4 of [Mo2], all $\mathbb{Z}\Gamma$-modules of this character are isomorphic to one of the following list:

- $\oplus_{j=1}^{q} P^{e_j}\mathfrak{a}_j \oplus \mathbb{S}$,
- $(\oplus_{j=1}^{l} P^{e_j}\mathfrak{a}_j, \mathbb{S}) \oplus_{j=l+1}^{q} P^{e_j}\mathfrak{a}_j$,

where $0 \leq e_j \leq q-1$ and the $\mathfrak{a}_j$ are ideal classes of $A_1 = \mathbb{Q}(\xi_p)^{\psi} \cap \mathbb{Z}[\xi_p]$ where ψ is the element of order q of the cyclic group $\mathrm{Gal}(\mathbb{Q}(\xi_p)/\mathbb{Q})$ and $(\oplus_{j=1}^{l} P^{e_j}\mathfrak{a}_j, \mathbb{S})$ represents a non-split extension of $\mathbb{S}$ by $\oplus_{j=1}^{l} P^{e_j}\mathfrak{a}_j$.

Let $u \in \mathbb{Z}$ be defined to be 0 if U_N is isomorphic to $\oplus_{j=1}^{q} P^{e_j}\mathfrak{a}_j \oplus \mathbb{S}$, and the number of distinct exponents e_j otherwise. We can define an invariant b of U_N to be $[U_K : N_{N/K}U_N]$ and theorem 2.3 of [Mo2] gives

$$b = [U_K : N_{N/K}U_N] = p^{q-1-u}. \tag{1.1}$$

Keep u as above and let

$$U_k \cong \oplus_{j=1}^{q} P_1^{\tilde{e_j}}\mathfrak{a}_j = \oplus_{j=1}^{q} P^{e_j} \cap A_1$$

then according to theorem 2.4 of [Mo2] there is a second invariant, a, of U_N given by

$$a = [U_N : U_k U_{k^\sigma} \dots U_{k^{\sigma^{q-1}}} U_K] = p^{\sum_{i=1}^{q}(q\tilde{e_i} - e_i) + u}. \tag{1.2}$$

Together a and b will not necessarily determine the genus of U_N except in the case where Γ is dihedral. Now let $N/\mathbb{Q}$ be a dihedral extension of order $2p$ with Galois group Γ. It is clear from the characters of U_N that there are two possibilities for the genus of U_N when N is complex, namely R and P, and five when N is real, namely $\mathbb{Z}^- \oplus R \oplus R$, $\mathbb{Z}^- \oplus R \oplus P$, $\mathbb{Z}^- \oplus P \oplus P$, $X \oplus R$, and $X \oplus P$.

Proposition 1.4. *([Mo1], III.3 and III.5) Let N be a real dihedral extension of order $2p$ of $\mathbb{Q}$.*

(i) If N is complex and

$$a = [U_N : U_k U_{k^\sigma}],$$

then the invariant a determines the genus of U_N in the following way:

U_N	a
R	1
P	p

(ii) If N is real and

$$a = [U_N : U_k U_{k^\sigma} U_K]$$
$$b = [U_K : N_{N/K} U_N]$$

where $N_{N/K}$ is the norm map, then the invariants a and b determine the genus of U_N in the following way:

Type	U_N	a	b
α	$\mathbb{Z}^- \oplus R \oplus R$	1	p
β	$\mathbb{Z}^- \oplus R \oplus P$	p	p
γ	$\mathbb{Z}^- \oplus P \oplus P$	p^2	p
δ	$X \oplus R$	p	1
ϵ	$X \oplus P$	p^2	1

□

To make it easier to calculate the invariant a we have the following proposition.

Proposition 1.5. *([Mol] IV.1) Let $N/\mathbb{Q}$ be dihedral of order $2p$, p an odd prime, then*

$$h_N = \frac{a\ h_k^2\ h_K}{p^r} \tag{1.3}$$

where $r = 1$ if N is complex and 2 if N is real. □

In the final section of [Mol] examples are calculated in the case when $p = 3$ for all cases of U_N except type α. In section 9.1 we shall give an example of this missing case.

Definition. Let N be a Galois extension of L with Galois group Γ, then we say N has a **Minkowski unit** if U_N is a cyclic $\mathbb{Z}\Gamma$-module.

This is equivalent to U_N being $\mathcal{A}_\Gamma$-isomorphic to $\mathcal{A}_\Gamma$.

Proposition 1.6. *([Mal], theorem 1) Let N be a real, metacyclic extension of $\mathbb{Q}$ of degree pm where p is a prime and $m|(p-1)$. If N has a Minkowski unit then*

$$h_K h_k^m = p^t h_N,$$

with $t \geq m-1$. $\square$

Proposition 1.7. *([Mal], theorem 2) Let N be a real, metacyclic extension of degree pq over $\mathbb{Q}$, where p and q are odd primes.*

(i) If N has a Minkowski unit, then there exists an ideal $\mathfrak{a} \lhd A_1$ and

(a) $U_N \cong X_{T^{max}} \oplus P\mathfrak{a}$,
where $\bar{T} = \{0, 2, 3, \ldots, q-1\}$,

(b) $\frac{h_K h_k^q}{h_N} = p^{q-1}$,

(c) $N_{N/K}(U_N) = U_K$,

(d) *the field K has a Minkowski unit.*

(ii) Conditions (b) and (c) are necessary and sufficient for U_N to be in the same genus as $\mathbb{Z}\Gamma/\mathbb{Z}T_\Gamma$.

(iii) If the class number of A_1 is 1, then (b),(c) and (d) are necessary and sufficient for K to have a Minkowski unit. Note that we can drop condition (d) if $q \leq 19$. $\square$

1.3. Notation.

N is a Galois extension of $\mathbb{Q}$ and L a subfield of N. Let $\Gamma = \mathrm{Gal(N/L)}$ be a metacyclic group of order pq.

$$\Gamma = \langle \sigma, \tau | \sigma^p = \tau^q = 1, \tau\sigma\tau^{-1} = \sigma^r \rangle$$

where p and q are distinct primes, p odd and $q|(p-1)$. r is a primitive qth root of unity modulo p. Whenever we use the words "pq-metacyclic group" we shall be referring to a group with this structure (i.e. not a pq-cyclic group.) When $q = 2$ then Γ is dihedral.

In general we shall try to use the notation Γ for a pq-metacyclic or dihedral group and G when we are referring to a general group.

Let $\mathcal{C}_p = \langle \sigma \rangle$ and $\mathcal{C}_q = \langle \tau \rangle$. Let K be the subfield of N fixed by $\mathcal{C}_p$ and k the subfield fixed by $\mathcal{C}_q$.

Let S be a Γ-invariant set of primes of N including

(i) all ramified primes,
(ii) all infinite primes and
(iii) enough primes so that the S-class group is cohomologically trivial.

Sometimes it may be necessary to add a fourth condition

(iv) S contains enough primes so that the S-class group of all intermediate fields between N and L is trivial.

Let S_∞ be the set of infinite primes of N and S_f be the set of finite primes in S. ΔS is the kernel of the augmentation map $\mathbb{Z}S \to \mathbb{Z}$, for any set S and $\hat{S}$ is the set of primes in L under those of S.

Let $\mathcal{E}_N$ be the units of N, and μ_N the roots of unity in N, and U_N be the torsion free units of N, i.e. $U_N \cong \mathcal{E}_N/\mu_N$. $\mathcal{E}_S$ are the S-units, and $U_S = \mathcal{E}_S/\mu_N$.

Let Cl_N be the class group of N and $h_N = |Cl_N|$ is the class number.

In general it is assumed that p does not divide the order of μ_N.

CHAPTER 2

Invariants for the genus of pq-metacyclic lattices.

Introduction.

The aim of this chapter is to find invariants determining the genus of a pq-metacyclic lattice in terms of other invariants which may be easier to calculate. In section 1.2 of the previous chapter we gave a list of genus representatives of the indecomposable pq-lattices. Now we would like to find a way to write a $\mathbb{Z}\Gamma$-lattice as a direct sum of these, in particular we would like to do this for the torsion-free units, U_N, of a pq-metacyclic extension, N.

In section 2.4 are some exact sequences which include the units. These give information on the cohomology of U_N. For a general group the cohomology of a lattice will give some information about the decomposition of that lattice. In the case when the group is pq-metacyclic the cohomology gives even more information about the genus. We shall show in section 2.3, theorem 2.6 that two lattices are in the same genus if and only if they have the same characters and cohomology.

Before this in section 2.1 is a list of some well known results on cohomology which will be used in this and later chapters. Then in section 2.2 we find the cohomology of pq-metacyclic lattices. In section 2.3 we calculate the invariants we will be using in later chapters to find the Galois module structure of the local units, S-units and global units. Finally we give some exact sequences including the cohomology of the units.

2.1. Cohomological results.

The results listed here for convenience are all either well known or simple corollaries to well known results.

2.1.1. Relations with Sylow p-subgroups.

Lemma 2.1. *Let Γ be any finite group, and let A be a Γ-module, then*

$$H^n(\Gamma, A) \cong \bigoplus_p H^n(\Gamma, A)_{(p)}, \tag{2.1}$$

where $H^n(\Gamma, A)_{(p)}$ is the p-primary component of $H^n(\Gamma, A)$, and p ranges over all the primes dividing $|\Gamma|$.

Proof. $H^n(\Gamma, A)$ is an Abelian group which is annihilated by $|\Gamma|$. $\square$

Definition. An inclusion $\Omega \hookrightarrow \Gamma$ and a Γ-module A induces a map

$$\mathrm{res}^{\Gamma}_{\Omega} : H^n(\Gamma, A) \to H^n(\Omega, A),$$

called the **restriction map**.

There is also a map between cohomology groups induced by conjugation. Let $\Omega \subseteq \Gamma$. Suppose $c(\gamma) : \Omega \to \gamma\Omega\gamma^{-1}$ for $\gamma \in \Gamma$, then there is a map

$$c(\gamma)^* : H^n(\gamma\Omega\gamma^{-1}, A) \to H^n(\Omega, A),$$

where A is a Γ-module.

Definition. If $z \in H^n(\Omega, A)$ then define

$$\gamma z = (c(\gamma)^*)^{-1}(z) \in H^n(\gamma\Omega\gamma^{-1}, A).$$

Definition. If $\Omega \subseteq \Gamma$ and A is a Γ-module then an element $z \in H^n(\Omega, A)$ is **Γ-invariant** if

$$\mathrm{res}^{\Omega}_{\Omega\cap\gamma\Omega\gamma^{-1}}(z) = \mathrm{res}^{\gamma\Omega\gamma^{-1}}_{\Omega\cap\gamma\Omega\gamma^{-1}}(\gamma z)$$

for all $\gamma \in \Gamma$.

Theorem 2.2. *([Br], p84, theorem 10.3) Let Γ be a finite group and $\Gamma_{(p)}$ a Sylow p-subgroup of Γ.*

(i) For any Γ-module A and any $n > 0$, $H^n(\Gamma, A)_{(p)}$ is isomorphic to the set of Γ-invariant elements of $H^n(\Gamma_{(p)}, A)$.

(ii) If $\Gamma_{(p)} \lhd \Gamma$ then $H^n(\Gamma, A)_{(p)} \cong H^n(\Gamma_{(p)}, A)^{\Gamma/\Gamma_{(p)}}$. $\square$

2.1.2. Cohomology of $\mathrm{Hom}(A, B)$.

Lemma 2.3. *([Br], p61, proposition 2.2) Let Γ be a finite group. If M is a $\mathbb{Z}\Gamma$-lattice, then*

$$\mathrm{Ext}^n_\Gamma(\mathrm{M}, \mathrm{A}) \cong \mathrm{H}^n(\Gamma, \mathrm{Hom}(\mathrm{M}, \mathrm{A}))$$

for any Γ-module A, where Γ acts diagonally on $\mathrm{Hom}(M, A)$. $\square$

Lemma 2.4. *([Br], p153, exercise 2) If A is a Γ-lattice and cohomologically trivial, then $\mathrm{Hom}(A, B)$ is cohomologically trivial for any Γ-module B.*

2.2. The cohomology of metacyclic groups.

2.2.1. Projective resolutions of $\mathbb{Z}$ for metacyclic groups.

Now let $\Gamma = \langle \sigma, \tau | \sigma^p = \tau^q = 1, \tau\sigma\tau^{-1} = \sigma^r \rangle$ where r is a primitive qth root of unity modulo p. In this section we shall find a projective resolution of $\mathbb{Z}$ for Γ of length $2q$. It can be shown that Γ has periodic cohomology of period $2q$, (see [Br], p155, example 3 for a proof using the fact that Γ has a $2q$-fixed-point-free representation) and so no shorter resolution is possible.

From lemma 2.1, for any Γ-module A

$$H^n(\Gamma, A) \cong H^n(\Gamma, A)_{(p)} \oplus H^n(\Gamma, A)_{(q)}. \tag{2.2}$$

Let $C_p = \langle \sigma \rangle$ and $C_q = \langle \tau \rangle$. $C_p \lhd \Gamma$ so by theorem 2.2(ii),

$$H^n(\Gamma, A)_{(p)} \cong H^n(C_p, A)^{C_q}$$

and by theorem 2.2(i), $H^n(\Gamma, A)_{(q)}$ is isomorphic to the Γ-invariant elements of $H^n(\mathcal{C}_q, A)$.

Firstly we show that all elements of $H^n(\mathcal{C}_q, A)$ are Γ-invariant. Now $\gamma\tau\gamma^{-1} \notin \mathcal{C}_q$ for $\gamma \in \Gamma \setminus \mathcal{C}_q$. So $\mathcal{C}_q \cap \gamma\mathcal{C}_q\gamma^{-1} = \{0\}$.

Thus both restriction maps are zero maps and hence are identical.

$$\begin{aligned}
\mathrm{res}^{\mathcal{C}_q}_{\mathcal{C}_q \cap \gamma\mathcal{C}_q\gamma^{-1}} &= \mathrm{res}^{\mathcal{C}_q}_{\{0\}} : H^n(\mathcal{C}_q, A) \to H^n(\{0\}, A) = 0, \\
\mathrm{res}^{\gamma\mathcal{C}_q\gamma^{-1}}_{\mathcal{C}_q \cap \gamma\mathcal{C}_q\gamma^{-1}} &= \mathrm{res}^{\gamma\mathcal{C}_q\gamma^{-1}}_{\{0\}} : H^n(\gamma\mathcal{C}_q\gamma^{-1}, A) \to H^n(\{0\}, A) = 0.
\end{aligned}$$

Therefore $\mathrm{res}^{\mathcal{C}_q}_{\mathcal{C}_q \cap \gamma\mathcal{C}_q\gamma^{-1}}(z) = 0 = \mathrm{res}^{\gamma\mathcal{C}_q\gamma^{-1}}_{\mathcal{C}_q \cap \gamma\mathcal{C}_q\gamma^{-1}}(\gamma z)$, for all $\gamma \in \Gamma$ and $z \in H^n(\mathcal{C}_q, A)$.

From the definition of Γ-invariance, since the restriction maps are the same,

$$H^n(\Gamma, A)_{(q)} \cong H^n(\mathcal{C}_q, A). \tag{2.3}$$

To calculate the Γ-cohomology groups it is necessary to find $\mathcal{C}_p$ and $\mathcal{C}_q$-projective Γ-exact resolutions of $\mathbb{Z}$. This is particularly easy in the $\mathcal{C}_q$-case.

Let $D = 1 - \tau$ and $N = 1 + \tau + \cdots + \tau^{q-1}$, then a $\mathcal{C}_q$-resolution of $\mathbb{Z}$ is

$$0 \leftarrow \mathbb{Z} \xleftarrow{\epsilon} \mathbb{Z}\mathcal{C}_q \xleftarrow{D_*} \mathbb{Z}\mathcal{C}_q \xleftarrow{N_*} \mathbb{Z}\mathcal{C}_q \xleftarrow{D_*} \cdots.$$

So that

$$H^n(\Gamma, A)_{(q)} \cong H^n(\mathcal{C}_q, A) \cong \begin{cases} \frac{\{a \mid \tau a = a, a \in A\}}{N^* A} & \text{when } n \text{ is even,} \\ \frac{\{a \mid Na = 0, a \in A\}}{D^* A} & \text{when } n \text{ is odd,} \end{cases}$$

and the q-part of the cohomology has period 2.

The p-part of the cohomology is more complicated because the 'normal' resolution of $\mathbb{Z}$ for a cyclic group, like the one used above, is not naturally a Γ-sequence. However, there are $2q$ short exact sequences

$$P_1 \to V \to \mathbb{Z}, \qquad \mathbb{Z} \to V \to P_0, \tag{2.4}$$
$$P_i \to X_{T^{\max}} \to X_{T_i^{\max}}, \qquad X_{T_i^{\max}} \to X_{T^{\max}} \to P_{i-1},$$

where $i \neq 1$, $T^{\max} = \{0, 2, 3, 4, \ldots, q-1\}$ and $X_{T_i^{\max}} = T^{\max} \setminus \{i\}$. These concatenate to give a long exact sequence of $2q+2$ terms

$$\mathbb{Z} \to V \to X_{T^{\max}} \to \cdots \to X_{T^{\max}} \to V \to \mathbb{Z}, \tag{2.5}$$

which concatenates with itself to give a $\mathbb{Z}C_p$-projective, $\mathbb{Z}\Gamma$-resolution of $\mathbb{Z}$ with period $2q$.

2.2.2. Cohomology with indecomposable lattice coefficients.

It is now possible to calculate the cohomology groups of metacyclic groups when the coefficients are indecomposable Γ-lattices.

Firstly the cohomology is calculated with $\mathbb{Z}$ as a coefficient. After some calculations we get

$$H^n(C_p, \mathbb{Z}) \cong \begin{cases} {\mathbb{F}_p}^{(n/2)} & n \text{ even,} \\ 0 & n \text{ odd,} \end{cases}$$

where ${\mathbb{F}_p}^{(a)}$ is cyclic of order p, and $\tau : {\mathbb{F}_p}^{(a)} \to {\mathbb{F}_p}^{(a)}$ by $\tau : f \mapsto r^a f$ for $f \in {\mathbb{F}_p}^{(a)}$ and r is a primitive qth root of 1 modulo p . Therefore, writing $\mathbb{F}_p$ and $\mathbb{F}_q$ for the cyclic groups of order p and q respectively,

$$H^n(\Gamma, \mathbb{Z})_{(p)} \cong \begin{cases} \mathbb{F}_p & n \equiv 0 \mod (2q) \\ 0 & \text{otherwise} \end{cases} \qquad H^n(\Gamma, \mathbb{Z})_{(q)} \cong \begin{cases} \mathbb{F}_q & n \text{ even} \\ 0 & n \text{ odd} \end{cases}$$

The short exact sequence $P \to V \to \mathbb{Z}$ and the fact V is C_p-projective give

$$H^n(C_p, P) \cong H^{n-1}(C_p, \mathbb{Z}).$$

The short exact sequence $P_i \to X_{T^{\max}} \to X_{T_i^{\max}}$ and the fact $X_{T^{\max}}$ is $\mathcal{C}_p$-projective give

$$H^n(\mathcal{C}_p, P_i) \cong H^{n-2}(\mathcal{C}_p, P_{i-1}) \qquad \text{for } i \neq 1.$$

We could continue in this way, finding isomorphisms between cohomology groups, to get the full cohomology of all the indecomposable lattices, listed below.

$$H^n(\Gamma, P_i)_{(p)} \cong \begin{cases} \mathbb{F}_p & n \equiv 2i-1 \mod (2q) \\ 0 & \text{otherwise} \end{cases} \qquad H^n(\Gamma, P_i)_{(q)} \cong 0 \quad \text{for all } n$$

$$H^n(\Gamma, \mathbb{S})_{(p)} \cong \begin{cases} \mathbb{F}_p & n \text{ even}, n \not\equiv 0 \mod (2q) \\ 0 & \text{otherwise} \end{cases} \qquad H^n(\Gamma, \mathbb{S})_{(q)} \cong \begin{cases} 0 & n \text{ even} \\ \mathbb{F}_q & n \text{ odd} \end{cases}$$

$$H^n(\Gamma, \mathbb{Z}\mathcal{C}_q)_{(p)} \cong \begin{cases} \mathbb{F}_p & n \text{ even} \\ 0 & n \text{ odd} \end{cases} \qquad H^n(\Gamma, \mathbb{Z}\mathcal{C}_q)_{(q)} \cong 0 \quad \text{for all } n$$

$$H^n(\Gamma, X_T)_{(p)} \cong \begin{cases} \mathbb{F}_p & n \equiv 2(t-1), t \notin T, t \neq 1 \\ 0 & \text{otherwise} \end{cases} \qquad H^n(\Gamma, X_T)_{(q)} \cong \begin{cases} 0 & n \text{ even} \\ \mathbb{F}_q & n \text{ odd} \end{cases}$$

$$H^n(\Gamma, Y_T)_{(p)} \cong \begin{cases} \mathbb{F}_p & n \equiv 2(t-1), t \notin T \\ 0 & \text{otherwise} \end{cases} \qquad H^n(\Gamma, Y_T)_{(q)} \cong 0 \quad \text{for all } n$$

$$H^n(\Gamma, V)_{(p)} \cong 0 \quad \text{for all } n \qquad H^n(\Gamma, V)_{(q)} \cong \begin{cases} \mathbb{F}_q & n \text{ even} \\ 0 & n \text{ odd} \end{cases}$$

where all congruences are modulo $2q$.

2.3. Invariants for the genus of metacyclic-lattices.

Let Γ be a pq-metacyclic group. Whilst the cohomology of any individual indecomposable Γ-lattice is unique to the lattices in that genus it is clear that direct sums of Γ-lattices can be arranged to have the same cohomology, even when they do not obviously lie in the same genus. It is also true that a lattice may not decompose uniquely into a direct sum of indecomposable lattices, however, we shall show in this section that these decompositions will still have the same cohomology. We shall in fact show that two Γ-lattices are in the same genus if and only if they have the same cohomology and characters.

Two Γ-lattices lie in the same genus if they have the same p-adic and q-adic completions. We shall show that the p-adic completion depends only on the cohomology and characters in proposition 2.5. This is done separately because we shall need this result when we look at extensions of local fields in chapter 3.

Proposition 2.5. *Let Γ be a metacyclic group of order pq. Let $\mathcal{M}$ be a Γ-lattice. Then the characters and p-part of the cohomology of $\mathcal{M}$ determine $\widehat{\mathcal{M}}$, the p-adic completion of $\mathcal{M}$.*

Note that in Chapter 7 we have used the notation $\mathcal{M}_p$ for p-adic completion.

Proof. Write $\mathcal{M}$ as a product of indecomposable Γ-modules

$$\mathcal{M} \vee \{ \bigoplus_i P_i^{r_i} \} \oplus \mathbb{Z}^{s_1} \oplus \mathbb{S}^{s_2} \oplus \mathbb{Z}C_q^l \oplus \{ \bigoplus_{T_1} X_{T_1}^{u_{T_1}} \} \oplus \{ \bigoplus_{T_2} Y_{T_2}^{v_{T_2}} \} \oplus V^w.$$

There are $3q$ indecomposable $\widehat{\mathbb{Z}}\Gamma$-lattices, namely (in the notation of [CR1]) $\widehat{P}_i, \widehat{\mathbb{Z}}_i$ and $\widehat{\mathbb{Z}^\Gamma}_i$ for $i = 1, \ldots, q$, and thus $\widehat{\mathcal{M}}$ is written as a product of these

$$\widehat{\mathcal{M}} = \{ \bigoplus_i \widehat{P}_i^{r_i} \} \oplus \widehat{\mathbb{Z}}_0^{s_1} \oplus \{\oplus_{i=1}^{q-1} \widehat{\mathbb{Z}}_i\}^{s_2} \oplus \{\oplus_{i=0}^{q-1} \widehat{\mathbb{Z}}_i\}^l \oplus$$
$$\{ \bigoplus_{T_1} [(\bigoplus_{t \in T_1} \widehat{\mathbb{Z}^\Gamma}_{t-1}) \oplus (\bigoplus_{t \notin T_1, t \neq 1} \widehat{\mathbb{Z}}_{t-1})]^{u_{T_1}} \} \oplus \{ \bigoplus_{T_2} [(\bigoplus_{t \in T_2} \widehat{\mathbb{Z}^\Gamma}_{t-1}) \oplus (\bigoplus_{t \notin T_2} \widehat{\mathbb{Z}}_{t-1})]^{v_{T_2}} \} \oplus \widehat{\mathbb{Z}^\Gamma}_0^w. \tag{2.6}$$

Note that $\mathbb{Z}^\Gamma$ comes from the non-split extension:

$$0/rightarrow \widehat{P}_i \to \widehat{\mathbb{Z}^\Gamma}_i \to \widehat{\mathbb{Z}}_i \to 0.$$

The number of times these indecomposable $\widehat{\mathbb{Z}}\Gamma$-lattices occur in $\widehat{\mathcal{M}}$ gives the following invariants of $\mathcal{M}$:

$$
\begin{array}{lrl}
\widehat{\mathbb{Z}}_0) & s_1 + l + \sum_{1 \notin T_2} v_{T_2} & = \alpha_0, \\
\widehat{\mathbb{Z}}_i) & s_2 + l + \sum_{i+1 \notin T_1} u_{T_1} + \sum_{i+1 \notin T_2} v_{T_2} & = \alpha_i, i \neq 0, \\
\widehat{\mathbb{Z}^{\Gamma}}_0) & \sum_{1 \in T_2} v_{T_2} + w & = \beta_0, \\
\widehat{\mathbb{Z}^{\Gamma}}_i) & \sum_{i+1 \in T_1} u_{T_1} + \sum_{i+1 \in T_2} v_{T_2} & = \beta_i, i \neq 0, \\
\widehat{P}_i) & r_i & = r_i.
\end{array}
$$

It is possible to write the invariants in terms of the cohomology and characters of $\mathcal{M}$ as claimed:

$$
\begin{aligned}
\text{No. of } \chi^+ \text{ in char}(\mathcal{M}) &= \alpha_0 + \beta_0, \\
\text{No. of } \chi^- \text{ in char}(\mathcal{M}) &= \alpha_i + \beta_i, \\
\log_p[H^{2i}(\Gamma, \mathcal{M})_{(p)}] &= \alpha_i, \\
\log_p[H^{2i-1}(\Gamma, \mathcal{M})_{(p)}] &= r_i,
\end{aligned}
$$

for $0 \leq i \leq q-1$. $\square$

If two lattices have the same cohomology and characters all that is now required to show they are in the same genus is show that they have the same q-adic completions (see [Pu]). However it is easier to follow the method in [CR1] and show that the lattices are the same when they are localized without completion at q rather than q-adically completed. This is the method used to prove the following theorem.

Theorem 2.6. *Let $\mathcal{M}$ be a Γ-lattice where Γ is a pq-metacyclic group. Then the characters and cohomology of $\mathcal{M}$ determine its genus.*

Proof. Write $\mathcal{M}$ as a product of indecomposable Γ-modules

$$
\mathcal{M} \vee \{ \bigoplus_i P_i^{r_i} \} \oplus \mathbb{Z}^{s_1} \oplus \mathbb{S}^{s_2} \oplus \mathbb{Z}C_q^l \oplus \{ \bigoplus_{T_1} X_{T_1}^{u_{T_1}} \} \oplus \{ \bigoplus_{T_2} Y_{T_2}^{v_{T_2}} \} \oplus V^w.
$$

From [CR1] §34E, the genus of $\mathcal{M}$ is determined by the indecomposable modules of $\mathcal{M}_{(q)}$ and $\widehat{\mathcal{M}}$, where the subscript (q) denotes localisation without completion and $\widehat{\mathcal{M}}$ is the p-adic completion of $\mathcal{M}$.

It has already been shown in proposition 2.5 that the characters and cohomology of $\mathcal{M}$ are enough to determine $\widehat{\mathcal{M}}$.

As for $\mathcal{M}_{(q)}$, there are four indecomposable $\mathbb{Z}_{(q)}\Gamma$-lattices, namely $R_{(q)}, \mathbb{Z}_{(q)}, S_{(q)}$, and $\mathbb{Z}_{(q)}\mathcal{C}_q$ and when $\mathcal{M}$ is localized at q without completion it becomes

$$\mathcal{M}_{(q)} = \{ \bigoplus_i R_{(q)}^{r_i} \} \oplus \mathbb{Z}_{(q)}^{s_1} \oplus \mathbb{S}_{(q)}^{s_2} \oplus \mathbb{Z}_{(q)}\mathcal{C}_q^{l} \oplus \{ \bigoplus_{T_1} (R_{(q)}^{|T_1|u_{T_1}} \oplus \mathbb{S}_{(q)}^{u_{T_1}}) \} \oplus$$
$$\{ \bigoplus_{T_2} (R_{(q)}^{|T_2|v_{T_2}}) \oplus \mathbb{Z}_{(q)}\mathcal{C}_q^{v_{T_2}} \} \oplus \{ R_{(q)} \oplus \mathbb{Z}_{(q)} \}^{w}.$$

The number of times these four indecomposable $\mathbb{Z}_{(q)}\Gamma$-lattices occur in $\mathcal{M}_{(q)}$ give four invariants of $\mathcal{M}$:

$$\begin{array}{lrl}
R_{(q)}) & \sum_i r_i + \sum_{T_1} |T_1| u_{T_1} + \sum_{T_2} |T_2| v_{T_2} + w & = \gamma, \\
\mathbb{Z}_{(q)}) & s_1 + w & = \delta, \\
\mathbb{S}_q) & s_2 + \sum_{T_1} u_{T_1} & = \varepsilon, \\
\mathbb{Z}_{(q)}\mathcal{C}_q) & l + \sum_{T_2} v_{T_2} & = \phi.
\end{array}$$

It is now possible write the invariants determining $\mathcal{M}_{(q)}$ in terms of the cohomology and characters of $\mathcal{M}$:

$$\begin{aligned}
\text{No. of } \chi^+ \text{ in char}(\mathcal{M}) &= \delta + \phi, \\
\text{No. of } \chi \text{ in char}(\mathcal{M}) &= \gamma, \\
\log_q H^{2i}(\Gamma, \mathcal{M})_{(q)} &= \delta, \\
\log_q H^{2i-1}(\Gamma, \mathcal{M})_{(q)} &= \varepsilon. \quad \square
\end{aligned}$$

For any finite group G it is possible in a similar way to tell when $\mathbb{Z}$ is a direct summand of a $\mathbb{Z}G$-lattice:

Theorem 2.7. *([Sy], theorem 1.1) Let G be any finite group and let $\mathcal{M}$ be a $\mathbb{Z}G$-lattice. Then $H^0(G, \mathcal{M})$ contains an element of order $|G|$ if and only if $\mathcal{M}$ contains the trivial $\mathbb{Z}G$-lattice, $\mathbb{Z}$, as a direct summand.* $\square$

For any finite group G, theorem 2.6 generally does not hold, but with a stronger condition on the isomorphisms between cohomology groups we can get a condition for two lattices $\mathcal{M}$ and $\mathcal{N}$ to be in the same genus.

Proposition 2.8. *Let $\mathcal{M}$ and $\mathcal{N}$ be G-lattices and*

$$f : \mathcal{M} \to \mathcal{N}$$

be a G-homomorphism so that

$$f^* : H^n(H, \mathcal{M}) \cong H^n(H, \mathcal{N}), \quad \forall n \in \mathbb{Z}, H \subseteq G,$$

and also $\mathbb{Q} \otimes \mathcal{M} \cong \mathbb{Q} \otimes \mathcal{N}$, then $\mathcal{M} \vee \mathcal{N}$.

Definition. Let $f, g \in \mathrm{Hom}_G(\mathcal{M}, \mathcal{N})$, then f is **homotopic** to g if $f - g$ factors through a projective $\mathbb{Z}G$-module and we write $f \sim g$.

Definition. $f : \mathcal{M} \to \mathcal{N}$ is a **homotopy equivalence** if there exists $g : \mathcal{N} \to \mathcal{M}$ such that $fg \sim id_N$ and $gf \sim id_M$. We write $\mathcal{M} \sim \mathcal{N}$.

Lemma 2.9. *([GW1], (10.1)) $\mathcal{M} \sim \mathcal{N}$ and $\mathbb{Q} \otimes \mathcal{M} \cong \mathbb{Q} \otimes \mathcal{N}$ implies $\mathcal{M} \vee \mathcal{N}$.* □

Lemma 2.10. *([GW1], (1.6)) The following statements about $f : \mathcal{M} \to \mathcal{N}$ are equivalent:*

(i) f is a homotopy equivalence,

(ii) there exists $\mathbb{Z}G$-projective modules P and Q and an isomorphism $\sigma : \mathcal{M} \oplus P \xrightarrow{\sim} \mathcal{N} \oplus Q$ so that f is the composite

$$\mathcal{M} \xrightarrow{i} \mathcal{M} \oplus P \xrightarrow{\sigma} \mathcal{N} \oplus Q \xrightarrow{\pi} \mathcal{N},$$

where i is the natural injection and π is the natural projection. □

Proof of proposition 2.8. Let f satisfy the conditions of proposition 2.8. By lemma 2.9 we will have proved the proposition if we show f is a homotopy equivalence. In fact, we shall show f satisfies condition (ii) of lemma 2.10.

Firstly, choose a projective presentation of $\mathcal{N}$, $\pi : P \twoheadrightarrow \mathcal{N}$ and form the short exact sequence

$$0 \to Q \longrightarrow \mathcal{M} \oplus P \xrightarrow{(f,\pi)} \mathcal{N} \to 0, \tag{2.7}$$

then $Q \subseteq \mathcal{M} \oplus P$ and both P and $\mathcal{M}$ are lattices so Q is too.

Take the cohomology of $H \subseteq G$ to get the exact sequence

$$\cdots \to H^n(H,Q) \to H^n(H,\mathcal{M} \oplus P) \xrightarrow{(f,\pi)^*} H^n(H,\mathcal{N}) \to \dots \tag{2.8}$$

$H^n(H,\mathcal{M} \oplus P) \cong H^n(H,\mathcal{M}) \overset{f^*}{\cong} H^n(H,\mathcal{N})$. So $H^n(H,Q) = 0$, thus Q is cohomologically trivial.

By [Br], p152 theorem (8.10) a cohomologically trivial lattice is projective. Therefore $\mathrm{Ext}^1_{\mathrm{G}}(\mathcal{N}, \mathrm{Q}) = 0$ and extension (2.7) splits.

Let $\nu : \mathcal{N} \to \mathcal{M} \oplus P$ be a splitting, then

$$\sigma : \mathcal{M} \oplus P = Q \oplus \nu(\mathcal{N}) \xrightarrow{\sim} Q \oplus \mathcal{N},$$

and this gives a factorisation of f as required. $\square$

2.4. Exact sequences for units.

Let U_N be the torsion-free units of the field N over L with Galois group Γ. The character of U_N is known, so from theorem 2.6 a knowledge of the cohomology of U_N would determine its genus. Throughout use $H^n(\Omega, -)$ to denote Tate cohomology, where Ω is a subgroup of Γ. The aim of this section is to derive an exact sequence to help calculate $H^n(\Omega, U_N)$.

Firstly, we get an exact sequence including $H^n(\Omega, \mathcal{E}_N)$ where $\mathcal{E}_N$ are the units of N.

Let S be a Γ-invariant set of primes in N. There is a short exact sequence

$$0 \to \mathcal{E}_N \to \mathcal{E}_S \to \mathcal{P}_S \to 0, \tag{2.9}$$

where $\mathcal{P}_S$ denotes the principal fractional ideals of N supported on the places in S_f and $\mathcal{E}_S$ are the S-units. Fixing under Ω gives a long exact sequence

$$0 \to \mathcal{E}_N^{\Omega} \to \mathcal{E}_S^{\Omega} \to \mathcal{P}_S^{\Omega} \to H^1(\Omega, \mathcal{E}_N) \to H^1(\Omega, \mathcal{E}_S) \to \dots \tag{2.10}$$

Next calculate $H^n(\Omega, \mathcal{E}_S)$ to substitute in (2.10). From [Ta], p.54, for S sufficiently large there is an exact sequence

$$0 \to \mathcal{E}_S \to A_3 \to B_3 \to \Delta S \to 0, \tag{2.11}$$

with A_3 and B_3 cohomologically trivial. Thus

$$H^n(\Omega, \Delta S) \cong H^{n+2}(\Omega, \mathcal{E}_S). \tag{2.12}$$

There exists another exact sequence including $H^n(\Omega, \mathcal{P}_S)$. Fixing the short exact sequence

$$0 \to \mathcal{P}_S \to \mathbb{Z}S_f \to Cl_N \to 0, \tag{2.13}$$

under Ω gives an exact sequence

$$0 \to \mathcal{P}_S^{\Omega} \to \mathbb{Z}S_f^{\Omega} \to Cl_N^{\Omega} \to H^1(\Omega, \mathcal{P}_S) \to 0 \to H^1(\Omega, Cl_N) \to H^2(\Omega, \mathcal{P}_S) \to \dots \tag{2.14}$$

since $H^1(\Omega, \mathbb{Z}S_f) = 0$.

The short exact sequence

$$0 \to \mu_N \to \mathcal{E}_N \to U_N \to 0, \tag{2.15}$$

gives a long exact sequence including $H^n(\Omega, U_N)$.

In particular, if $p \nmid |\mu_N|$ for some rational prime p then

$$H^n(\Omega, \mathcal{E}_N)_{(p)} \cong H^n(\Omega, U_N)_{(p)}. \tag{2.16}$$

Simplifications.

Note that if we assume $H^n(\Omega, Cl_N)_{(p)} = 0$, (e.g. if p does not divide the class number) then clearly

$$H^n(\Omega, \mathcal{P}_S)_{(p)} \cong H^n(\Omega, \mathbb{Z}S_f)_{(p)}. \tag{2.17}$$

We can add another condition to those on page 17, (iv) S contains enough primes so that the S-class number of all intermediate fields between N and L is 1, then

$$H^1(\Omega, \mathcal{E}_S) = 0. \tag{2.18}$$

(This comes from the exact sequences

$$\begin{array}{ccccccccccc}
0 & \to & \mathcal{E}_{S,N^\Omega} & \to & (N^\Omega)^* & \to & \mathcal{I}_{S,N^\Omega} & \to & Cl_{S,N^\Omega} & \to & 0 \\
 & & \| & & \| & & \downarrow & & \downarrow & & \text{(by Hilbert 90)} \\
0 & \to & \mathcal{E}^\Omega_{S,N} & \to & (N^*)^\Omega & \to & \mathcal{I}^\Omega_{S,N} & \to & H^1(\Omega, \mathcal{E}_{S,N}) & \to & H^1(\Omega, N^*) = 0
\end{array}$$

where $\mathcal{I}_S$ are the ideals prime to S and the second subscript indicates which field the modules come from.)

CHAPTER 3

Principal units of metacyclic extensions of local fields.

Introduction.

Before looking at the global units we shall in this chapter study the simpler local case. Firstly we give some previous results on units of local extensions in the general case (see [GW1], [GW2]) and for metacyclic extensions (see [Ja2], [Ja3]). Then we shall use the results we found in the last chapter to look at some cases that these papers do not cover.

3.1. Previous work on units of local extensions.

Let N/L be a Galois extension of local fields with Galois group G and residue field of characteristic p. Let $\mathcal{U}$ be the units of N, and $\mathcal{U}_1$ be the principal units. [GW1] give conditions determining the isomorphism class of $\mathcal{U}_1$. Before writing this result (theorem 3.1) it is necessary to define a Γ-module, W, and give some notation.

Definition. Let $\mathfrak{P}$ be the maximal ideal of N. The **principal units**, $\mathcal{U}_1$ is the multiplicative group of units congruent to 1 modulo $\mathfrak{P}$.

The exact sequence which defines the units $\mathcal{U}$ of N is

$$0 \to \mathcal{U} \to N^\times \xrightarrow{\nu} \mathbb{Z} \to 0, \tag{3.1}$$

where ν is the normalized valuation.

As explained in [GW1] there exists an exact sequence

$$0 \to N^\times \to V \to \Delta G \to 0,$$

with V cohomologically trivial, this comes from the Tate sequence for local units

$$0 \to N^\times \to A \to B \to \mathbb{Z} \to 0.$$

Form the pushout along ν:

$$\begin{array}{ccccc}
\mathcal{U} & = & \mathcal{U} & & \\
\downarrow & & \downarrow & & \\
N^\times & \longrightarrow & V & \longrightarrow & \Delta G \\
\downarrow \nu & & \downarrow & & \downarrow = \\
\mathbb{Z} & \longrightarrow & W & \longrightarrow & \Delta G
\end{array}$$

Thus we get

$$0 \to \mathcal{U} \to V \to W \to 0 \tag{3.2}$$

with V cohomologically trivial ([GW1], §12.)

By [GW1], theorem (12.3), W is given by the pullback square

$$\begin{array}{ccc}
W & \longrightarrow & \Delta G \\
\downarrow & & \downarrow - \\
\mathbb{Z}\overline{G} & \xrightarrow[F-1]{} & \Delta \overline{G}
\end{array}$$

where $-$ is the canonical map $G \to \overline{G}$ to the Galois group of the residue extension field and F in $\overline{G}$ is the Frobenius automorphism.

The elements of W are pairs $(x, y) \in \Delta G \oplus \mathbb{Z}\overline{G}$ such that $\overline{x} = (F-1)y$. Let

$$\widehat{W} = \widehat{\mathbb{Z}} \otimes_{\mathbb{Z}} W.$$

The split exact sequence

$$0 \to \mathcal{U}_1 \to \mathcal{U} \to \overline{N^\times} \to 0, \tag{3.3}$$

where $\overline{N}$ is the residue field of N, implies $\mathcal{U}_1$ is a finitely generated $\widehat{\mathbb{Z}}G$-module and $\mathcal{U}_1$ is the p-completion of $\mathcal{U}$.

Taking the p-completion of (3.2) gives

$$0 \to \mathcal{U}_1 \to \widehat{V} \to \widehat{W} \to 0$$

of finitely generated $\widehat{\mathbb{Z}}G$-modules. $\widehat{V}$ is cohomologically trivial.

Theorem 3.1. *([GW1], theorem 13.3) The $\widehat{\mathbb{Z}}G$-module $\mathcal{U}_1$ is determined up to isomorphism by the following invariants*

(i) *the degree $[L : \widehat{\mathbb{Q}}]$,*

(ii) *the G-module $\mu_N(p)$ of p-power roots of unity in N,*

(iii) *the kernel of the map*

$$H^1(G, \mathrm{Hom}(\widehat{W}, \mu_N(p)) \to H^1(G, \mathrm{Hom}(\widehat{W}, \mathcal{U}_1))$$

induced by the inclusion $\mu_N(p) \hookrightarrow \mathcal{U}_1$. $\square$

Definition. Let $\mathcal{M}$ be a $\widehat{\mathbb{Z}}G$-module, if $\mathcal{M} = \mathcal{M}' \oplus C$ where C is cohomologically trivial and $\mathcal{M}'$ has no cohomologically trivial summand, then $\mathcal{M}'$ is called the **strict core** of $\mathcal{M}$. It is unique up to isomorphism (by the Krull-Schmidt theorem.)

Theorem 3.2. *([GW2], theorem 6.1) The strict core of $\mathcal{U}$ is*

(a) *zero if p does not divide the ramification index, e,*

(b) *non-zero and indecomposable if p divides e provided we are not in the exceptional case when p does not divide f, the inertial degree of N/L, and at least one of the maps*

$$H^1(G, \mathrm{Hom}(\widehat{\mathbb{Z}}, \mu_N(p))) \to H^1(G, \mathrm{Hom}(\widehat{\mathbb{Z}}, \mathcal{U}_1)),$$

$$H^1(G, \mathrm{Hom}(\hat{\Delta}G, \mu_N(p))) \to H^1(G, \mathrm{Hom}(\hat{\Delta}G, \mathcal{U}_1)),$$

induced by the inclusion $\mu_N(p) \hookrightarrow \mathcal{U}_1$, is zero,

(c) *the direct sum of two non-zero indecomposable modules in the exceptional case.*

$\square$

Moving on to the metacyclic case. Let $N/\mathbb{Q}_p$ be a metacyclic extension of local fields with Galois group Γ. Let Γ be metacyclic of order pm where m is a non-trivial divisor of $p-1$, not necessarily prime.

It has been necessary in other chapters to make m a prime because otherwise it is possible for Γ to have infinite representation type, however, in the local case we are looking at $\widehat{\mathbb{Z}}\Gamma$-lattices and there are still $3m$ indecomposable genera of these whether or not m is a prime.

In [Ja1], Jaulent calculates the indecomposable $\widehat{\mathbb{Z}}\Gamma$-lattices and their cohomology groups. These calculations agree with those in Chapter 2 and it is clear that we can re-write proposition 2.5 to include the cases when m is not prime:

Proposition 3.3. *Let Γ be a metacyclic group of order pm. If $\widehat{\mathcal{M}}$ is a $\widehat{\mathbb{Z}}\Gamma$-lattice and*

$$\widehat{\mathcal{M}} = \bigoplus_{i=0}^{m-1}((\widehat{\mathbb{Z}}_i)^{\alpha_i} \oplus (\widehat{\mathbb{Z}^{\Gamma}}_i)^{\beta_i} \oplus (\widehat{P}_i)^{r_i}),$$

(see the proof of proposition 2.5 for a definition of these lattices) then we can find α_i, β_i and r_i from the characters and p-part of the cohomology of $\widehat{\mathcal{M}}$ in exactly the same way as in the proof of proposition 2.5.

$$\begin{aligned} \alpha_i &= \log_p[H^{2i}(\Gamma, \mathcal{M})_{(p)}], \\ r_i &= \log_p[H^{2i-1}(\Gamma, \mathcal{M})_{(p)}], \\ \alpha_0 + \beta_0 &= \textit{No. of } \chi^+ \textit{ in } \mathrm{char}\mathcal{M}, \\ \alpha_i + \beta_i &= \textit{No. of } \chi^- \textit{ in } \mathrm{char}\mathcal{M},\ \mathrm{i} \neq 0, \end{aligned}$$

for $0 \le i \le m-1$. $\square$

One way of indexing the $3m$ indecomposable $\widehat{\mathbb{Z}}\Gamma$-lattices is by the irreducible p-adic characters of $\mathcal{C}_m$, call these $\phi_o, \ldots \phi_{m-1}$. Then the lattices are as follows:

$$\widehat{\mathbb{Z}^{\Gamma}_{\phi_i}} = \widehat{\mathbb{Z}}[\mathcal{C}_p].e_{\phi_i}$$
$$\widehat{P_{\phi_i}} = \widehat{\mathbb{Z}^{\Gamma}_{\phi_i}}/v\widehat{\mathbb{Z}^{\Gamma}_{\phi_i}}$$
$$\widehat{\mathbb{Z}_{\phi_i}} = \widehat{\mathbb{Z}^{\Gamma}_{\phi_i}}/\theta\widehat{\mathbb{Z}^{\Gamma}_{\phi_i}}$$

where e_{ϕ_i} is the idempotent $e_{\phi_i} = 1/m \sum_{\tau \in \mathcal{C}_m} \phi_i(\tau^{-1})\tau$ and $v = 1+\sigma+\cdots+\sigma^{p-1}$. Let χ be the primitive p-adic character of $\mathcal{C}_m$ defined by $\tau\eta\tau^{-1} = \eta^{\chi(\tau)}$ for all $\tau \in \mathcal{C}_m, \eta \in \mathcal{C}_p$, then $\theta = 1/m \sum_{\tau \in \mathcal{C}_m} \chi(\tau^{-1})\sigma^{\chi(\tau)}$.

Let $\mathfrak{P}$ be the maximal ideal of N. For all integers $k \geq 1$ let $\mathcal{U}_k$ be the multiplicative group of principal units congruent to 1 modulo $\mathfrak{P}^k$.

In [Ja3], Jaulent finds all k where $\frac{\mathcal{U}_k/\mu_N}{N_{N/K}(\mathcal{U}_k)}$ is free over the algebra $\Lambda = \widehat{\mathbb{Z}}[\xi \circ \mathcal{C}_m]$, ($\xi$ is defined below) and finds the $\widehat{\mathbb{Z}}\Gamma$-module structure of $\mathcal{U}_k$ in these cases.

Let e be the ramification index of p in $K = N^{\mathcal{C}_p}$ and let t be the jump of wild ramification, which satisfies

$$t \leq \left[\frac{ep}{p-1}\right]$$

Let ξ be a principal unit of $\mathcal{U}$ that is in $\mathcal{U}_t$ but not in $\mathcal{U}_{t+1}$.

Theorem 3.4. *([Ja3], theorem 3) Let $K = N^{\mathcal{C}_p}$ contain no pth roots of unity, then $\mathcal{U}_k/N_{N/K}(\mathcal{U}_k)$ is free over Λ if and only if the cohomology groups of $\mathcal{U}_k$ relative to $\mathcal{C}_p$ have the same character Φ; this happens exactly in the following cases:*

(i) *in tame ramification - for all values of k,*
(ii) *in wild ramification - for all k of the form $r + p\mathbb{N}$ where $r \in [1,p]$ which satisfies $r \equiv 1 \mod (e)$,*

and in these cases $\mathcal{U}_k$ is written as the direct sum

$$\mathcal{U}_k \cong \{ \bigoplus_{\phi_i | \Phi} (\widehat{P_{\phi_i}} \oplus \widehat{\mathbb{Z}_{\phi_i}})\} \oplus \{ \bigoplus_{\phi_i \nmid \Phi} \widehat{\mathbb{Z}^{\Gamma}_{\phi_i}}\}. \quad \square$$

Theorem 3.5. *([Ja3], theorem 4) Let K contain pth roots of unity, then $\frac{\mathcal{U}_k/\mu_N}{N_{N/K}(\mathcal{U}_k)}$ is free over Λ for $k = 1, \ldots, p$ if and only if the cohomology groups of $\mathcal{U}_k/\mu_N$ relative to $\mathcal{C}_p$ have the same character Ω; this happens exactly in the following cases:*

(i) $k = p - 1$,

(ii) $k = 1$,

and in these cases $\mathcal{U}_k/\mu_N$ is written as the direct sum

$$\mathcal{U}_k/\mu_N \cong \{ \bigoplus_{\phi_i|\Omega} (\widehat{P_{\phi_i}} \oplus \widehat{\mathbb{Z}_{\phi_i}})\} \oplus \{ \bigoplus_{\phi_i\nmid\Omega} \widehat{\mathbb{Z}_{\phi_i}^{\Gamma}}\}. \quad \square$$

In the next section we shall find the decomposition of $\mathcal{U}_1$ when N is a metacyclic extension of L for any local field L. Note that $\mathcal{U}_1$ is always free over Λ and so the case $L = \mathbb{Q}_p$ has already been done, but we shall look at general L and find that the genus of $\mathcal{U}_1$ depends only on whether or not N contains pth power roots of unity. We shall also look at $\mathcal{U}_k$ for larger k.

3.2. The Galois module structure of local units.

Let N be a metacyclic extension of local fields of degree pq over L with Galois group Γ. Both p and q are prime. Let L be of degree d over $\widehat{\mathbb{Q}}$.

Proposition 3.6. *Let $\mathcal{U}$ be the units of N, then*

$$H^n(\Gamma, \mathcal{U})_{(p)} \cong \begin{cases} \mathbb{F}_p & n \equiv 1,2 \mod (2q), \\ 0 & \textit{otherwise.} \end{cases}$$

Proof. There is a short exact sequence

$$0 \to N^\times \to V \to \Delta\Gamma \to 0, \tag{3.4}$$

with V cohomologically trivial (see [GW1], theorem 11.3.)

Thus the cohomology of $N^\times$ is determined by

$$H^n(\Gamma, \Delta\Gamma) \cong H^{n+1}(\Gamma, N^\times).$$

The short exact sequence (3.1) gives a long exact sequence

$$\cdots \to H^n(\Gamma,\mathcal{U}) \to H^n(\Gamma,N^\times) \to H^n(\Gamma,\mathbb{Z}) \to \dots \tag{3.5}$$

Now the cohomology of $N^\times$ is clear because

$$H^n_{(p)}(\Gamma,N^\times) \cong H^{n-1}_{(p)}(\Gamma,\Delta\Gamma) \cong H^{n-1}_{(p)}(\Gamma,X_{T^{\max}} \oplus P_1) \cong \begin{cases} \mathbb{F}_p & \text{if } n \equiv 2 \mod (2q), \\ 0 & \text{otherwise.} \end{cases}$$

This and the cohomology of $\mathbb{Z}$ put into the sequence (3.5) give the required result. □

Theorem 3.7. *Let N be a pq-metacyclic extension of local fields over L and L is of degree d over $\widehat{\mathbb{Q}}$. Let $\mathcal{U}_1$ be the principal units of N.*

(i) *Suppose N contains no pth roots of unity. Then*

$$\mathcal{U}_1 \vee \widehat{P_1} \oplus \widehat{\mathbb{Z}}_1 \oplus (\widehat{\mathbb{Z}^{\Gamma}}_1)^{d-1} \oplus (\bigoplus_{i\neq 1, i=0}^{q-1} \widehat{\mathbb{Z}^{\Gamma}}_i)^d \tag{3.6}$$

(ii) *If L contains pth roots of unity then*

$$\frac{\mathcal{U}_1}{\mu_N(p)} \vee \widehat{P}_0 \oplus \widehat{P}_1 \oplus \widehat{\mathbb{Z}}_1 \oplus \widehat{\mathbb{Z}}_{q-1} \oplus (\widehat{\mathbb{Z}^{\Gamma}}_1)^{d-1} \oplus (\widehat{\mathbb{Z}^{\Gamma}}_{q-1})^{d-1} \oplus (\bigoplus_{i\neq 1, i=0}^{q-2} \widehat{\mathbb{Z}^{\Gamma}}_i)^d. \tag{3.7}$$

Proof. We know that $\widehat{\mathbb{Q}} \otimes \mathcal{U}_1 \cong N \cong \widehat{\mathbb{Q}} \otimes \widehat{\mathbb{Z}}(\Gamma^d)$. So

$$\mathrm{char}(\mathcal{U}_1) = \mathrm{d}(\mathrm{char}\Gamma) = \mathrm{d}(\chi^+ + \chi^- + \mathrm{q}\chi).$$

(i) Suppose now that N contains no pth root of unity. Then it is clear that the characters of $\mathcal{U}_1$ and the cohomology of $\mathcal{U}_1$ are the same as those of $\mathcal{U}$ by sequence (3.3). Since $\mathcal{U}_1$ is torsion-free it is a $\mathbb{Z}_p\Gamma$-lattice and we can now determine its genus.

(ii) If N contains pth roots of unity, then L also contains these units.

Thus $\mu_N(p)$ is fixed under Γ. $\mu_N(p)$ is cyclic of order p^r with trivial Γ-action. So the cohomology is

$$H^n(\Gamma, \mu_N(p)) \cong \begin{cases} \mathbb{F}_p & \text{if } n \equiv 0, 2q-1 \mod (2q), \\ 0 & \text{otherwise.} \end{cases}$$

We have a long exact sequence

$$\cdots \to H^n(\Gamma, \mu_N(p)) \to H^n(\Gamma, \mathcal{U}) \to H^n(\Gamma, \mathcal{U}/\mu_N(p)) \to \ldots.$$

So for $p \neq 3$ we have

$$H^n(\Gamma, \mathcal{U}/\mu_N(p)) \cong \begin{cases} \mathbb{F}_p & n \equiv 1, 2, 2q-1, 2q-2 \mod (2q), \\ 0 & \text{otherwise.} \end{cases} \tag{3.8}$$

Thus we know the cohomology and characters of the p-adic lattice $\mathcal{U}_1/\mu_N(p)$ and we know its genus. □

Higher order local units.

Let $\mathfrak{P}$ be the maximal ideal of N and let $\mathcal{U}_k$ be the multiplicative group of principal units congruent to 1 modulo $\mathfrak{P}^k$.

We have short exact sequences for all $k \geq 1$

$$0 \to \mathcal{U}_{k+1} \to \mathcal{U}_k \to \mathfrak{P}^k/\mathfrak{P}^{k+1} \to 0. \tag{3.9}$$

Lemma 3.8. *Let N be a local extension of L with galois group Γ then*

$$H^n(\Gamma, \mathfrak{P}^k/\mathfrak{P}^{k+1}) \cong \begin{cases} \mathbb{F}_p & n \equiv 2ka-1, 2ka \mod (2q) \\ 0 & \textit{otherwise.} \end{cases}$$

for some $0 \leq a \leq q-1$.

If $\Gamma_0 = \mathcal{C}_p$ then $a = 0$.

Proof. Let Γ_1 be the first ramification group and $\Gamma_1 \cong \mathcal{C}_p$ which acts trivially on $\mathfrak{P}^k/\mathfrak{P}^{k+1}$. There is a non-trivial action of $\Gamma_0/\Gamma_1 \cong \mathcal{C}_q$ on $\mathfrak{P}^k/\mathfrak{P}^{k+1}$.

Write $\mathfrak{P} = \pi\mathcal{O}_N$, then

$$\tau : \pi \to r^a\pi.$$

where r is a primitive qth root of $1 \mod (p)$ (r comes from the definition of Γ in section 1.3.)

Thus $\mathfrak{P}/\mathfrak{P}^2 \cong \mathbb{F}_p^{(a)}$ for some a and so

$$\mathfrak{P}^k/\mathfrak{P}^{k+1} \cong \mathbb{F}_p^{(ka)}.$$

(see section 2.2.2 for a definition of $\mathbb{F}_p^{(a)}$.) This gives the cohomology given. $\square$

Proposition 3.9. *Let N be a pq-metacyclic extension of L of local fields and let L have degree d over $\widehat{\mathbb{Q}}$. Let $\mathcal{U}_2$ be the multiplicative group of principal units congruent to 1 modulo $\mathfrak{P}^2$. If N contains no pth roots of unity and the inertia group of p is $\mathcal{C}_p$ then $\mathcal{U}_2$ is isomorphic to:*

$$\widehat{\mathbb{Z}_0} \oplus \widehat{\mathbb{Z}_1} \oplus \widehat{P_1}^2 \oplus \widehat{(\mathbb{Z}_0^\Gamma)}^{d-1} \oplus \widehat{(\mathbb{Z}_1^\Gamma)}^{d-1} \oplus (\bigoplus_{i=2}^{q-1} \widehat{\mathbb{Z}_i^\Gamma})^d$$

Proof. If we now suppose that N contains no pth roots of unity then we know the cohomology of $\mathcal{U}_1$ (proposition 3.6) and $\mathfrak{P}^1/\mathfrak{P}^2$ (lemma 3.8) so we can get an exact sequence from (3.9)

$$0 \to H^0(\Gamma, \mathcal{U}_2) \to \mathbb{F}_p \to \mathbb{F}_p \to H^1(\Gamma, \mathcal{U}_2) \to \mathbb{F}_p \to \mathbb{F}_p \to H^2(\Gamma, \mathcal{U}_2) \to 0$$

and

$$H^i(\Gamma, \mathcal{U}_2) \cong 0 \quad i \not\equiv 0, 1, 3 \mod (2q).$$

Thus there is are the only one possibility for the cohomology groups:

$$H^0(\Gamma, \mathcal{U}_2) = H^2(\Gamma, \mathcal{U}_2)\mathbb{F}_p \text{ and } H^1(\Gamma, \mathcal{U}_2) = \mathbb{F}_p \oplus \mathbb{F}_p,$$

which gives respectively the decomposition given in the proposition, of $\mathcal{U}_2$ as a product of indecomposable $\widehat{\mathbb{Z}}\Gamma$-lattices. $\square$

CHAPTER 4

The S-units.

Introduction.

The Tate sequence, equation (2.11), gives the cohomology of the S-units, $\mathcal{E}_S$, and thus it is easy to give possibilities for the cohomology of the torsion-free S-units, U_S. We also know the character of U_S and this means we can apply theorem 2.6 to find its genus (see section 4.3). We also need to calculate the cohomology of $\mathcal{E}_S$ in order to find the cohomology of the units.

Before doing this we look at [GW1] where Gruenberg and Weiss give an invariant, $\mathcal{U}$ which can be used to determine when two modules are in the same genus. For pq-metacyclic groups we find the cases when there is only one choice for $\mathcal{U}$ and these turn out to be the cases in the final section where we can calculate U_S exactly.

4.1. An invariant for S-units.

Let N/L be any finite extension of number fields with Galois group G, where G is any finite group. Let S be a G-invariant set of primes containing the infinite and ramified primes and let $\mathcal{E}_S$ be the S-units of N. $U_S = \mathcal{E}_S/\mu_N$ where μ_N are the torsion units of $\mathcal{E}_S$.

Define $\mathcal{U}$ to be the kernel of the map

$$H^2(G, \mathrm{Hom}(\Delta S, \mu_N)) \to H^2(G, \mathrm{Hom}(\Delta S, \mathcal{E}_S))$$

induced by $\mu_N \hookrightarrow \mathcal{E}_S$.

Gruenberg and Weiss, [GW1] give a way of determining when a Γ-module $\mathcal{E}'$ is in the same genus as $\mathcal{E}_S$.

Theorem 4.1. *([GW1], (10.2)) Let $\mathcal{E}'$ be a $\mathbb{Z}G$-module satisfying the following conditions:*

(i) $\mathbb{Q} \otimes \mathcal{E}' \cong \mathbb{Q} \otimes \Delta S$ as $\mathbb{Q}G$-modules;

(ii) $\mathcal{E}'$ has $\mathbb{Z}$-torsion submodule G-isomorphic to μ_N;

(iii) there exists an exact sequence of $\mathbb{Z}G$-modules

$$0 \to \mathcal{E}' \to C' \to P' \to \Delta S \to 0,$$

where C' is cohomologically trivial and P' is projective;

(iv) $\mathcal{U} = \mathcal{U}'$, where $\mathcal{U}'$ is the kernel of

$$H^2(G, \mathrm{Hom}(\Delta S, \mu_N)) \to H^2(G, Hom(\Delta S, \mathcal{E}'))$$

induced by $\mu_N \hookrightarrow \mathcal{E}'$.

Then $\mathcal{E}'$ and $\mathcal{E}_S$ are in the same genus. $\square$

4.2. The Module $H^2(G, \mathrm{Hom}(\Delta S, \mu_N))$.

It is of interest to determine the invariant $\mathcal{U}$ of the S-units. In particular, when $H^2(G, \mathrm{Hom}(\Delta S, \mu_N)) = 0$ then there is only one choice for $\mathcal{U}$.

From the short exact sequence

$$0 \to \Delta S \to \mathbb{Z}S \to \mathbb{Z} \to 0, \tag{4.1}$$

we get a long exact sequence for $H^2(G, \mathrm{Hom}(\Delta S, \mu_N))$

$$\begin{aligned} \ldots \to H^2(G, \mathrm{Hom}(\mathbb{Z}, \mu_N)) \to H^2(G, \mathrm{Hom}(\mathbb{Z}S, \mu_N)) \to \\ H^2(G, \mathrm{Hom}(\Delta S, \mu_N)) \to H^3(G, \mathrm{Hom}(\mathbb{Z}, \mu_N)) \to \ldots \end{aligned} \tag{4.2}$$

Now $\mathbb{Z}S \cong \bigoplus_{\pi \in \hat{S}} \mathbb{Z}[G/\mathcal{L}_\pi]$ where $\mathcal{L}_\pi$ is the decomposition group of Π, for $\pi \in \hat{S}, \Pi$ in N lying above π in L.

$$H^n(G, \mathrm{Hom}(\mathbb{Z}S, \mu_N)) \cong \bigoplus_{\pi \in \hat{S}} H^n(\mathcal{L}_\pi, \mu_N).$$

Let q be any rational prime such that q divides $|\mu_N|$. $\mathcal{L}_\pi$ = decomposition group of Π lying above $\pi \in \hat{S}$.

The three possible cases are:

Case 1. $q \nmid |\mathcal{L}_\pi|, \forall \pi \in \hat{S}$

Proposition 4.2. *If* $q \nmid |\mathcal{L}_\pi|, \forall \pi \in \hat{S}$ *then*

$$H^2(G, \mathrm{Hom}(\Delta S, \mu_N))_{(q)} \cong H^3(G, \mu_N)_{(q)}, \tag{4.3}$$

where the subscript (q) *means* q*-primary component.* $\square$

This follows from the long exact sequence (4.2).

Corollary 1. *Therefore, if* $q \nmid |\mathcal{L}_\pi|$*, for all primes* $\pi \in \hat{S}$ *and for all rational primes* q *dividing* $|G|$*, then*

$$H^2(G, \mathrm{Hom}(\Delta S, \mu_N)) \cong H^3(G, \mu_N). \quad \square \tag{4.4}$$

Corollary 2. *If* $\gcd(|G|, |\mu_N|) = 1$ *, then*

$$H^2(G, \mathrm{Hom}(\Delta S, \mu_N)) \cong 0. \quad \square \tag{4.5}$$

Case 2. $S_q \subseteq \mathcal{L}_{\pi j}$ for some $\pi_j \in \hat{S}, S_q$ a q-Sylow subgroup of G.

Proposition 4.3. *If* $S_q \subseteq \mathcal{L}_{\pi j}$ *for some* $\pi_j \in \hat{S}, S_q$ *a* q*-Sylow subgroup of* G *then*

$$H^2(G, \mathrm{Hom}(\Delta S, \mu_N))_{(q)} \cong_{\pi \in \hat{S} \setminus \pi_j} \bigoplus H^2(\mathcal{L}_\pi, \mu_N)_{(q)}. \tag{4.6}$$

Proof.

$$H^n(G, \mu_N)_{(q)} \cong H^n(\mathcal{L}_{\pi j}, \mu_N)_{(q)},$$

by [Se], p119, proposition and the result follows using the long exact sequence (4.2).

$\square$

Corollary 1. *If* $\mathcal{L}_{\pi j} \cong G$ *for some* $\pi \in \hat{S}$ *then*

$$H^2(G, \mathrm{Hom}(\Delta S, \mu_N)) \cong \bigoplus_{\pi \in S \setminus \pi_j} H^2(\mathcal{L}_\pi, \mu_N). \quad \square \tag{4.7}$$

Corollary 2. *So if* $\mathcal{L}_{\pi j} \cong G$ *for some* $\pi_j \in \hat{S}$ *,* $\gcd(|\mathcal{L}_\pi|, |\mu_N|) = 1, \forall \pi \in \hat{S} \setminus \pi_j$ *then*

$$H^2(G, \mathrm{Hom}(\Delta S, \mu_N)) \cong 0. \quad \square \tag{4.8}$$

Case 3. $q||\mathcal{L}_{\pi j}|$ for some $\pi_j \in S$, but $S_q \not\subseteq \mathcal{L}_\pi, \forall \pi \in S$.
In this case it is difficult to say anything about $H^2(\mathrm{Hom}(\Delta S, \mu_N))$ and since it does not occur when G is dihedral we shall not study it.

Example 1. $|G| = q_1 q_2 \ldots q_m$ distinct primes.

Case 3 never occurs and all q-Sylow subgroups are cyclic. Suppose q_i divides $|\mathcal{L}_{\pi j}|$ for some $\pi_j \in \hat{S}$ for $1 \leq i \leq k$ and $q_i \nmid |\mathcal{L}_\pi|$ for all $\pi \in \hat{S}$ for $k+1 \leq i \leq m$. i.e. we order the primes so that the first k divide $|\mathcal{L}_\pi|$ for some $\pi \in \hat{S}$ and the remainder do not.

Then simply putting together the results of Cases 1 and 2

$$H^2(G, \mathrm{Hom}(\Delta S, \mu_N)) \cong$$
$$\{\bigoplus_{k+1 \leq i \leq m, \pi \in S \setminus \pi_j} H^2(\mathcal{L}_\pi, \mu_N)_{(q_i)}\}\} \oplus \{\bigoplus_{q_i, k+1 \leq i \leq m} \{H^3(G, \mu_N)_{(q_i)}\}\},$$

where the q_i range over all the rational primes dividing $|G|$.

Example 2. Metacyclic groups.

Let $G = \mathcal{C}_p \rtimes \mathcal{C}_q$ be a metacyclic group of order pq.

If $\gcd(|G|, |\mu_N|) = 1$ then $H^n(G, \mathrm{Hom}(\Delta S, \mu_N)) = 0$ and thus $\mathcal{U} = 0$.

If $\gcd(|G|, |\mu_N|) = q$ and q divides $|\mathcal{L}_\pi|$ for some prime π then we are in Case 2.

So $q||\mathcal{L}_{\pi j}|$ for some $\pi_j \in \hat{S}$, implying $H^2(G, \mathrm{Hom}(\Delta S, \mu_N)) \cong \bigoplus_{\pi \in S \setminus \pi_j} H^2(\mathcal{L}_\pi, \mu_N)$. and $\#\{\pi \in \hat{S} \setminus \pi_j | q \text{ divides } |\mathcal{L}_\pi|\} = \#\{\mathcal{L}_\pi \cong \mathcal{C}_q \text{ or } G | \pi \in \hat{S}\} - 1 = \beta$.

So $H^2(G, \mathrm{Hom}(\Delta S, \mu_N)) \cong \mathbb{F}_q^{\beta}$.

Finally, if $\gcd(|G|, |\mu_N|) = q$ and q did not divide $\mathcal{L}_\pi$ for any prime π then we are in Case 1. Thus

$$H^2(G, \mathrm{Hom}(\Delta S, \mu_N)) \cong H^3(G, \mu_N) \cong \mathbb{F}_q.$$

Note. Thus there are two cases where the invariant $\mathcal{U}$ is guaranteed to be 0:

(i) $\gcd(|G|, |\mu_N|) = 1$,
(ii) $\gcd(|G|, |\mu_N|) = q$ and $\#\{\pi \in \hat{S} | \mathcal{L}_\pi \cong C_q \text{ or } G\} = 1$.

In these two cases, given μ_N there is only one possibility for the genus of $\mathcal{E}_S$, and hence U_S. We shall calculate U_S in these two cases in proposition 4.6.

4.3. Cohomology with S-unit coefficients.

4.3.1. Galois module structure of S-units.

Let N/L be a Galois extension with Galois group Γ where Γ is a metacyclic group of order pq. S is a set of Γ-invariant primes containing the ramified and infinite primes as before.

Lemma 4.4. *Let S be a set of primes fixed under Γ, and let $\mathcal{L}_\pi$ be the decomposition group of $\pi \in \hat{S}$, then*

$$\mathbb{Z}S \cong \bigoplus_{\pi \in \hat{S}} \mathbb{Z}[\mathcal{L}_\pi \backslash \Gamma],$$

and if $\mathcal{L}_{\pi_i} \subseteq \mathcal{L}_{\pi_j}$ for some $\pi_i \neq \pi_j \in \hat{S}$ then

$$\Delta S \cong \mathbb{Z}[\mathcal{L}_{\pi_i} \backslash \Gamma] \oplus \Delta S',$$

for $S' = S \setminus \pi_i$.

Proof. Let $\bar{e}_k$ be the class of the identity of Γ in $\mathcal{L}_{\pi_k}\backslash\Gamma$. Then $\langle \bar{e}_i - \bar{e}_j\rangle \cong \mathcal{L}_{\pi_i}\backslash\Gamma$ as a Γ-module and is also in the kernel of the augmentation map: $\mathbb{Z}S \to \mathbb{Z}$. $\square$

Let $\hat{S}$ have m_1 primes with decomposition group $\{0\}$, m_2 with $\mathcal{C}_q$, m_3 with $\mathcal{C}_p$ and m_4 with Γ. Then

$$\mathbb{Z}S \cong \mathbb{Z}\Gamma^{m_1} \oplus \mathbb{Z}[\mathcal{C}_q \setminus \Gamma]^{m_2} \oplus \mathbb{Z}[\mathcal{C}_p \setminus \Gamma]^{m_3} \oplus \mathbb{Z}^{m_4}$$

and we have the following isomorphisms of Γ-modules:

$$\begin{aligned} &\mathbb{Z}[\{1\} \setminus \Gamma] \cong Y_{T^{\max}} && \\ &\mathbb{Z}[\mathcal{C}_q \setminus \Gamma] \cong V && \Delta[\mathcal{C}_q \setminus \Gamma] \cong P \\ &\mathbb{Z}[\mathcal{C}_p \setminus \Gamma] \cong \mathbb{Z}\mathcal{C}_q && \Delta[\mathcal{C}_p \setminus \Gamma] \cong \mathbb{S} \\ &\mathbb{Z}[\Gamma \setminus \Gamma] \cong \mathbb{Z} && \Delta[\mathcal{C}_q \setminus \Gamma, \mathcal{C}_p \setminus \Gamma] \cong Y_{\{1\}} \end{aligned} \tag{4.9}$$

where $Y_{\{1\}}$ means $T = 1$ in the notation given in section 1.2.

Recall that S_f is the set of finite primes of S, so

$$\mathbb{Z}S_f \cong \begin{cases} Y_{T^{\max}}^{m_1-d} \oplus V^{m_2} \oplus \mathbb{Z}\mathcal{C}_q^{m_3} \oplus \mathbb{Z}^{m_4-1} & \text{if } N \text{ is totally real or complex over complex,} \\ Y_{T^{\max}}^{m_1} \oplus V^{m_2-d} \oplus \mathbb{Z}\mathcal{C}_q^{m_3} \oplus \mathbb{Z}^{m_4-1} & \text{if } N \text{ is complex over real.} \end{cases}$$

It is now possible to calculate the cohomology of $\mathbb{Z}S_f$ to substitute into equation (2.14)

$$H^n(\Gamma, \mathbb{Z}S_f) \cong \begin{cases} \mathbb{F}_q^{m_2+(-d)+m_4} \oplus \mathbb{F}_p^{m_3+m_4} & n \equiv 0 \mod (2q), \\ \mathbb{F}_q^{m_2+(-d)+m_4} \oplus \mathbb{F}_p^{m_3} & n \text{ even}, n \not\equiv 0 \mod (2q), \\ 0 & \text{otherwise,} \end{cases}$$

where d is subtracted when N is complex and not if N is real.

As for the cohomology of the S-units, equation (2.12) says $H^n(\Omega, \Delta S) \cong H^{n+2}(\Omega, \mathcal{E}_S)$.

Case A. When $m_3 = m_4 = 0$,

$$\Delta S \cong Y_T^{m_1} \oplus V^{m_2-1} \oplus P,$$

and so the cohomology of ΔS is

$$H^n(\Gamma, \Delta S) \cong \begin{cases} \mathbb{F}_q^{m_2-1} & n \text{ even}, \\ \mathbb{F}_p & n \equiv 1 \mod (2q), \\ 0 & \text{otherwise}. \end{cases} \tag{4.10}$$

Case B. When $m_3 + m_4 \geq 1$,

$$\Delta S \cong \begin{cases} Y_{\bar{T}}^{m_1} \oplus V^{m_2} \oplus \mathbb{Z}C_q^{m_3} \oplus \mathbb{Z}^{m_4-1}, & m_4 \geq 1, \\ Y_{\bar{T}}^{m_1} \oplus V^{m_2-1} \oplus \mathbb{Z}C_q^{m_3-1} \oplus Y_{\{1\}}, & m_4 = 0, \end{cases}$$

and so the cohomology of ΔS is

$$H^n(\Gamma, \Delta S) \cong \begin{cases} \mathbb{F}_q^{m_2+m_4-1} \oplus \mathbb{F}_p^{m_3+m_4-1} & n \equiv 0 \mod (2q), \\ \mathbb{F}_q^{m_2+m_4-1} \oplus \mathbb{F}_p^{m_3} & n \text{ even}, n \not\equiv 0 \mod (2q), \\ 0 & \text{otherwise}. \end{cases} \tag{4.11}$$

which gives us the cohomology of $\mathcal{E}_S$ by equation (2.13).

Proposition 4.5. *Let N be a pq-metacyclic extension of L with Galois group Γ and S a Γ-invariant set of primes of N as before.*

Let $\hat{S}$ be the primes of L below those in S and let $\hat{S}$ have m_3 primes with decomposition group C_p and m_4 with Γ. Then clearly the number of primes ramifying in N over N^{C_p} is less than or equal to $m_3 + m_4$. Let U_S be the torsion-free S-units.

$$m_3 + m_4 = 0 \textit{ implies } U_S \vee P_2 \oplus (Y_{T_2^{max}})^{m_1} \oplus V^{m_2-1}$$
$$\textit{or } P_2 \oplus (Y_{T_2^{max}})^{m_1-1} \oplus X_{T_1^{max}} \oplus V^{m_2}$$
$$m_3 + m_4 \geq 1 \textit{ implies } U_S \vee \mathbb{Z}C_q^{m_3} \oplus (Y_{T^{max}})^{m_1-m_4+1} \oplus {Y_{T_2^{max}\setminus\{2\}}}^{m_4-1} \oplus V^{m_2+m_4-1}$$
$$\textit{or } \mathbb{Z}C_q^{m_3} \oplus X_{T_1^{max}} \oplus (Y_{T_2^{max}})^{m_1-m_4} \oplus {Y_{T_2^{max}\setminus\{2\}}}^{m_4-1} \oplus V^{m_2+m_4}$$

where $T_1^{max} = \{0, 2, 3, \ldots, q-1\}$ and $T_2^T = \{0, 1, 2, \ldots, q-1\}$

Proof. We have a short exact sequence

$$0 \to \mu_N \to \mathcal{E}_S \to U_S \to 0,$$

which gives a long exact sequence

$$\cdots \to H^n(\Gamma, \mu_N) \to H^n(\Gamma, \mathcal{E}_S) \to H^n(\Gamma, U_S) \to \ldots$$

As usual $\gcd(p, |\mu_N|) = 1$ so $H^n(\Gamma, U_S)_{(p)} \cong H^n(\Gamma, \mathcal{E}_S)_{(p)} \cong H^{n-2}(\Gamma, \Delta S)_{(p)}$ and clearly we get different values depending on whether $m_3 + m_4$ is zero or not.

The torsion units, μ_N, form a cyclic Γ-module which means that $H^n(\Gamma, \mu_N)_{(q)} \cong 0$ if $\gcd(q, |\mu_N|) = 1$, or if $\gcd(q, |\mu_N|) = q$ and the action of Γ on the q-part is non-trivial (i.e. if and only if L contains a primitive qth root of 1). Otherwise we have $H^n(\Gamma, \mu_N)_{(q)} \cong \mathbb{F}_q$ (clearly this is always the case if $q = 2$). we just calculated gives two possible values for the cohomology of U_S. when $H^n(\Gamma, \mu_N)_{(q)} \cong \mathbb{F}_q$. The long exact sequence above becomes

$$0 \to H^{2n-1}(\Gamma, U_S)_{(q)} \to \mathbb{F}_q \to \mathbb{F}_q^{m_2+m_4-1} \to H^{2n}(\Gamma, U_S)_{(q)} \to \mathbb{F}_q \to 0$$

So, either

$$H^n(\Gamma, U_S)_{(q)} \cong \begin{cases} 0 & n \text{ odd} \\ \mathbb{F}_q^{m_2+m_4-1} & n \text{ even} \end{cases}$$

or

$$H^n(\Gamma, U_S)_{(q)} \cong \begin{cases} \mathbb{F}_q & n \text{ odd} \\ \mathbb{F}_q^{m_2+m_4} & n \text{ even} \end{cases}$$

Recall that the q-part of the cohomology is periodic of period 2, so this cohomology applies for all n.

Since $\Delta S \otimes \mathbb{Q} \cong U_S \otimes \mathbb{Q}$ we also know that $char(U_S) = (m_1 + m_2 + m_3 + m_4 - 1)\chi^+ + (m_1 + m_3)\chi^- + (qm_1 + m_2)\chi$ and thus by theorem 2.6 know the genus of U_S. □

Proposition 4.6. *When $\mathcal{U} = 0$ there is only one possible genus for U_S (as discussed in the previous section), thus* *(i) If* $\gcd(q, |\mu_N|) = 1$ *then*

$$m_3 + m_4 = 0 \textit{ implies } U_S \vee P_2 \oplus (Y_{T^{max_2}})^{m_1} \oplus V^{m_2-1}$$

$$m_3 + m_4 \geq 1 \textit{ implies } U_S \vee \mathbb{Z}\mathcal{C}_q^{m_3} \oplus (Y_{T^{max_2}})^{m_1-m_4+1} \oplus Y^{m_4-1}_{T^{max}\setminus\{2\}} \oplus V^{m_2+m_4-1}.$$

(ii) If $\gcd(q, |\mu_N|) = q$ *and* $m_2 + m_4 = 1$ *then*

$$m_3 + m_4 = 0 \textit{ implies } U_S \vee P_2 \oplus (Y_{T^{max_2}})^{m_1-1} \oplus X_{T^{max_1}} \oplus V$$

$$m_3 + m_4 \geq 1 \textit{ implies } U_S \vee \mathbb{Z}\mathcal{C}_q^{m_3} \oplus X_{T^{max_1}} \oplus (Y_{T^{max_2}})^{m_1-m_4} \oplus Y^{m_4-1}_{T^{max_2}\setminus\{2\}} \oplus V$$

Proof. (i)$\gcd(q, |\mu_N|) = 1$ implies that $\gcd(\Gamma, |\mu_N|) = 1$, since we always assume $\gcd(p, |\mu_N|) = 1$. So we get $H^n(\Gamma, \mathcal{E}_S) \cong H^n(\Gamma, U_S)$.

(ii) $m_2 + m_4 = 1$ implies $H^n(\Gamma, \mathcal{E}_S)_{(q)} = 0$ for all n. So
$H^n(\Gamma, U_S)_{(q)} \cong H^n(\Gamma, \mu_N)_{(q)} \cong \mathbb{F}_q$ as μ_N is a trivial, cyclic Γ-module. □

4.3.2. Exact sequences.

Lemma 4.7. *The S-class group can be made cohomologically trivial by adding completely split primes to S.*

Hence it is possible to choose a set of primes S satisfying coditions (i) to (iii) of section 1.3 containing only the ramified, infinite and completely split primes.

Proof. From the Tchebotarev density theorem each ideal class of the class group has Dirichlet density $1/h_N$, so each ideal class contains infinitely many completely split primes. □

Note. If the set of primes S is chosen to satisfy condition (iv) given in Chapter 1 (and thus $H^1(\Omega, \mathcal{E}_S) \cong H^{-1}(\Omega, \Delta S) = 0$ for all n) then $m_3 + m_4 \geq 1$. This is clear from the cohomology of the lattices in ΔS. Condition (iv) implies that $H^1(\mathcal{C}_p, \mathcal{E}_S) = 0$. Now $H^1(\mathcal{C}_p, \mathcal{E}_S) \cong H^{-1}(\mathcal{C}_p, \Delta S)$ and $H^{-1}(\mathcal{C}_p, \Delta S) = 0$ if and only if $m_3 + m_4 \neq 0$. Thus it may be necessary to add non-ramified primes with decomposition group $\mathcal{C}_p$ to S.

Knowing the cohomology of $\mathbb{Z}S_f$ (see (4.10) and (4.11)) means we can write down more information on the exact sequence (2.14)

$$0 \to \mathcal{P}_S^\Gamma \to \mathbb{Z}S_f{}^\Gamma \to Cl_N^\Gamma \to H^1(\Gamma, \mathcal{P}_S) \to 0, \tag{4.12}$$

$$\begin{aligned} 0 \to H^{2n-1}(\Gamma, Cl_N) \to H^{2n}(\Gamma, \mathcal{P}_S) \to \mathbb{F}_q^{m_2+(-d)+m_4} \oplus \mathbb{F}_p^{m_3+m_4} \\ \to H^{2n}(\Gamma, Cl_N) \to H^{2n+1}(\Gamma, \mathcal{P}_S) \to 0, \quad n \equiv 0 \mod (q), \end{aligned} \tag{4.13}$$

$$\begin{aligned} 0 \to H^{2n-1}(\Gamma, Cl_N) \to H^{2n}(\Gamma, \mathcal{P}_S) \to \mathbb{F}_q^{m_2+(-d)+m_4} \oplus \mathbb{F}_p^{m_3} \\ \to H^{2n}(\Gamma, Cl_N) \to H^{2n+1}(\Gamma, \mathcal{P}_S) \to 0 \quad n \not\equiv 0 \mod (q). \end{aligned} \tag{4.14}$$

With this new information on the value of the cohomology groups the exact sequence (2.10) becomes

$$0 \to \mathcal{E}_N^\Gamma \to \mathcal{E}_S^\Gamma \to \mathcal{P}_S^\Gamma \to H^1(\Gamma, \mathcal{E}_N) \to 0. \tag{4.15}$$

Case A. When $m_3 = m_4 = 0$

$$\begin{aligned} 0 \to H^{2n-1}(\Gamma, \mathcal{P}_S) \to H^{2n}(\Gamma, \mathcal{E}_N) \to \mathbb{F}_q^{m_2-1} \\ \to H^{2n}(\Gamma, \mathcal{P}_S) \to H^{2n+1}(\Gamma, \mathcal{E}_N) \to 0, \quad n \not\equiv 1,2 \mod (q), \end{aligned} \tag{4.16}$$

$$\begin{aligned} 0 \to H^{2n-1}(\Gamma, \mathcal{P}_S) \to H^{2n}(\Gamma, \mathcal{E}_N) \to \mathbb{F}_q^{m_2-1} \\ \to H^{2n}(\Gamma, \mathcal{P}_S) \to H^{2n+1}(\Gamma, \mathcal{E}_N) \to \mathbb{F}_p \to H^{2n+1}(\Gamma, \mathcal{P}_S) \to H^{2n+2}(\Gamma, \mathcal{E}_N) \to \mathbb{F}_q^{m_2-1} \\ \to H^{2n+2}(\Gamma, \mathcal{P}_S) \to H^{2n+3}(\Gamma, \mathcal{E}_N) \to 0, \quad n \equiv 1 \mod (q). \end{aligned} \tag{4.17}$$

Case B. When $m_3 + m_4 \geq 1$

$$\begin{aligned} 0 \to H^{2n-1}(\Gamma, \mathcal{P}_S) \to H^{2n}(\Gamma, \mathcal{E}_N) \to \mathbb{F}_q^{m_2+m_4-1} \oplus \mathbb{F}_p^{m_3+m_4-1} \\ \to H^{2n}(\Gamma, \mathcal{P}_S) \to H^{2n+1}(\Gamma, \mathcal{E}_N) \to 0, \quad n \equiv 1 \mod (q), \end{aligned} \tag{4.18}$$

$$0 \to H^{2n-1}(\Gamma, \mathcal{P}_S) \to H^{2n}(\Gamma, \mathcal{E}_N) \to \mathbb{F}_q^{m_2+m_4-1} \oplus \mathbb{F}_p^{m_3}$$
$$\to H^{2n}(\Gamma, \mathcal{P}_S) \to H^{2n+1}(\Gamma, \mathcal{E}_N) \to 0, \quad n \not\equiv 1 \mod (q). \quad (4.19)$$

CHAPTER 5

Cl_N and ramified primes with decomposition group $\mathcal{C}_p$.

Introduction.

In Chapter 6 we shall study the Galois module structure of the units when the p-part of the class group is trivial, i.e. $(Cl_N)_{(p)} = 0$. We shall show that in this case there are no ramified primes with decomposition group $\mathcal{C}_p$ (see theorem 5.5). This will simplify the calculations required to find the genus of U_N, but first we shall give a list in proposition 5.3 of the possible decompositions of a prime ideal in N.

5.1. Decomposition of primes in metacyclic extensions.

Let $\Gamma = \mathrm{Gal(N/L)}$ be a metacyclic group of order pq. Let

$$\mathcal{L}_\pi = \{\gamma \in \Gamma | \gamma(\Pi_i) = \Pi_i, \Pi \text{ an ideal of } N \text{ above } \pi \text{ of } L\},$$

be the decomposition group of the prime π in N/L. Let $\bar{N_i} = N/\Pi_i = \bar{N}$ and $\bar{L} = L/\pi$, which are finite fields. The following two lemmas are proved in [Ri], Chapter 11, for example.

Lemma 5.1. *There is a homomorphism $\mathcal{L}_\pi \to \mathrm{Gal}(\bar{\mathrm{N}}/\bar{\mathrm{L}})$ with kernel $\mathcal{T}_\pi$, the inertial group of π and $|\mathcal{T}_\pi| = e_\pi$, the ramification index of π.*

So $\mathcal{T}_\pi$ is a normal subgroup of $\mathcal{L}_\pi$. □

Lemma 5.2. *(i) Let $\mathcal{V}_1$ be the first ramification group of π in N/L, then $\mathcal{V}_1$ is a normal subgroup of $\mathcal{T}_\pi$ and $\mathcal{T}_\pi/\mathcal{V}_1$ is cyclic.*

(ii) The order of $\mathcal{V}_1$ is a power of the rational prime s where $s = \pi \cap \mathbb{Z}$. □

Proposition 5.3. *(i) There are 7 possible decompositions of a prime ideal $\pi \in L$ as a product of prime ideals in N, namely,*

$$\begin{aligned} (\pi) &= \Pi^{pq}, & (\pi) &= \Pi_1 \dots \Pi_{pq}, \\ (\pi) &= \Pi^{p}, & (\pi) &= \Pi_1 \dots \Pi_{q}, \\ (\pi) &= \Pi_1{}^{p} \dots \Pi_q{}^{p}, & (\pi) &= \Pi_1 \dots \Pi_{p}, \\ (\pi) &= \Pi_1{}^{q} \dots \Pi_p{}^{q}, \end{aligned}$$

(ii) If $(\pi) = \Pi^{pq}$ then π lies over p.

Proof. (i) There are eight possible cases where $\mathcal{T}_\pi \mathcal{L}_\pi \subset \Gamma$, but the case $\mathcal{L}_\pi = \Gamma$ and $\mathcal{T}_\pi = \{e\}$ does not occur because that would imply by lemma 5.1, $\Gamma \subset \mathrm{Gal}(\bar{\mathrm{N}}/\bar{\mathrm{L}})$, and $\mathrm{Gal}(\bar{\mathrm{N}}/\bar{\mathrm{L}})$ is Abelian, so this is impossible.

(ii) Let $\mathcal{T}_\pi = \Gamma$ and $\mathcal{L}_\pi = \Gamma$. By lemma 5.2 (i), $\mathcal{T}_\pi/\mathcal{V}_1$ is cyclic so $\mathcal{V}_1 \neq \{e\}$. Thus $\mathcal{V}_1 = \mathcal{C}_p$ but the order of $\mathcal{V}_1$ is a power of $s = \pi \cap \mathbb{Z}$ by lemma 5.2 (ii), so $p = s$. □

5.2. Cl_N and ramified primes with decomposition group $\mathcal{C}_p$.

Lemma 5.4. *([Ge], p487, lemma 2) Let* Gal(N/$\mathbb{Q}$) *be the dihedral group of order* 6. *If π is a rational prime which ramifies in N with decomposition group $\mathcal{C}_3$ then $3|h_N$, where h_N is the class number of N.*

From this lemma we see there is a relationship between the class group and the ramified primes with decomposition group $\mathcal{C}_p$ when $p = 3$ and $q = 2$. We now generalise this in theorem 5.5 for pq-metacyclic extensions over $\mathbb{Q}$ and also write down a specific formula for m_3', the number of primes with ramification group $\mathcal{C}_p$, in terms of Γ-cohomology groups of the class group.

Theorem 5.5. *Let N be a metacyclic extension of $\mathbb{Q}$ with pq-metacyclic Galois group Γ, then*

$$p^{m_3'} = \frac{|Cl_N^\Gamma|_{(p)} \times |H^{-1}(\Gamma, Cl_N)|_{(p)}}{|H^0(\Gamma, Cl_N)|_{(p)}}. \tag{5.1}$$

Thus, if at least one prime in $\mathbb{Q}$ ramifies in N with decomposition group C_p then p divides the class number h_N.

Proof. Let S satisfy conditions (i) to (iii) of section 1.3. It is assumed that at least one prime ramifies over N/K, i.e. $m_3+m_4 \geq 1$. All the groups in the exact sequences (4.18) and (4.13) are finite and so we can use (4.13) with $n=0$ to calculate the order of $H^1(\Omega, \mathcal{P}_S)$

$$|H^1(\Omega, \mathcal{P}_S)| = \frac{|H^0(\Omega, \mathcal{P}_S)| \times |H^0(\Omega, Cl_N)|}{|H^{-1}(\Omega, Cl_N)| \times |H^0(\Omega, \mathbb{Z}S_f)|}, \tag{5.2}$$

and use (4.19) with $n=0$ to substitute for $|H^0(\Omega, \mathcal{P}_S)|$ in the above equation. Thus one equation giving the order of $H^1(\Omega, \mathcal{P}_S)$ is

$$|H^1(\Omega, \mathcal{P}_S)| = \frac{|H^1(\Omega, \mathcal{E}_N)| \times |H^0(\Omega, Cl_N)| \times |H^{-1}(\Omega, \mathcal{P}_S)| \times |H^0(\Omega, \mathcal{E}_S)|}{|H^{-1}(\Omega, Cl_N)| \times |H^0(\Omega, \mathcal{E}_N)| \times |H^0(\Omega, \mathbb{Z}S_f)|}. \tag{5.3}$$

Alternatively $|H^1(\Omega, \mathcal{P}_S)|$ can be calculated by using the exact sequence (2.14). Since $H^1(\Omega, \mathbb{Z}S_f) = 0$ for all $\Omega \subset \Gamma$ we could re-write (2.14) as

$$0 \to \mathbb{Z}S_f^{\Omega}/\mathcal{P}_S^{\Omega} \to Cl_N^{\Omega} \to H^1(\Omega, \mathcal{P}_S) \to 0,$$

and thus

$$|H^1(\Omega, \mathcal{P}_S)| = \frac{|Cl_N^{\Omega}|}{[\mathbb{Z}S_f{}^{\Omega} : \mathcal{P}_S^{\Omega}]}. \tag{5.4}$$

Since $H^1(\Omega, \mathcal{E}_S) = 0$ for all $\Omega \subset \Gamma$ we can arrange (2.10) to say

$$0 \to \mathcal{E}_S^{\Omega}/\mathcal{E}_N^{\Omega} \to \mathcal{P}_S^{\Omega} \to H^1(\Omega, \mathcal{E}_N) \to 0,$$

and thus

$$|H^1(\Omega, \mathcal{E}_N)| = [\mathcal{P}_S^{\Omega} : \mathcal{E}_S^{\Omega}/\mathcal{E}_N^{\Omega}]. \tag{5.5}$$

Also there is an exact sequence in N^{Ω}

$$0 \to \mathcal{E}_{N^{\Omega}} \to \mathcal{E}_{S,N^{\Omega}} \to \mathbb{Z}S_{f,N^{\Omega}} \to Cl_{N^{\Omega}} \to 0, \tag{5.6}$$

where the second subscript shows which field we are working in and we get

$$|Cl_{N^\Omega}| = [\mathbb{Z}S_{f,N^\Omega} : \mathcal{E}_{S,N^\Omega}/\mathcal{E}_{N^\Omega}]. \tag{5.7}$$

Now $\mathcal{E}_S^\Omega = \mathcal{E}_{S,N^\Omega}$ and $\mathcal{E}_N^\Omega = \mathcal{E}_{N^\Omega}$ so substituting (5.7) and (5.5) into (5.4) gives a second way of calculating the order of $H^1(\Omega, \mathcal{P}_S)$

$$|H^1(\Omega, \mathcal{P}_S)| = \frac{|Cl_N^\Omega| \times |H^1(\Omega, \mathcal{E}_N)|}{|Cl_{N^\Omega}| \times [\mathbb{Z}S_f{}^\Omega : \mathbb{Z}S_{f,N^\Omega}]}. \tag{5.8}$$

Remark. Equation (5.8) does not depend on $m_3 + m_4 = 0$, unlike equation (5.3).

The inclusion $\mathbb{Z}S_{f,N^\Omega} \hookrightarrow \mathbb{Z}S_f{}^\Omega$ is given by $\pi \mapsto e_\pi tr_\Omega(\pi)$ where e_π is the ramification index of π in the extension N/N^Ω and $tr_\Omega(\pi) = \sum_{\Pi|\pi} \Pi, \Pi \in \mathbb{Z}S_f$.

As before we write S_L as $\hat{S}$, let $\Omega = \Gamma$ and look at the p-part of equation (5.8). Then $[\mathbb{Z}S_f{}^\Gamma : \mathbb{Z}\hat{S}_f]_{(p)} = p^{m_3'+m_4'}$, where m_3' is the number of *ramified* primes with decomposition group $\mathcal{C}_p$ and m_4' is the number of ramified primes with decomposition group Γ. (Note that $m_4' = m_4$ because from proposition 5.3 all the primes with decomposition group Γ ramify to at least the power p).

Equating the p-parts of (5.3) and (5.8), noting that

$$p^{m_4} \times |H^0(\Gamma, \mathcal{E}_S)|_{(p)} = |H^0(\Gamma, \mathbb{Z}S_f)|_{(p)},$$

(from the cohomology of $\mathcal{E}_S$ and $\mathbb{Z}S_f$ given in the previous chapter) and rearranging, gives

$$p^{m_3'} = \frac{|Cl_N^\Gamma|_{(p)} \times |H^{-1}(\Gamma, Cl_N)|_{(p)} \times |H^0(\Gamma, \mathcal{P}_S)|_{(p)}}{|Cl_L|_{(p)} \times |H^0(\Gamma, Cl_N)|_{(p)} \times |H^{-1}(\Gamma, \mathcal{E}_N)|_{(p)}}. \tag{5.9}$$

If $L = \mathbb{Q}$ then $Cl_L = \{0\}$ and $H^0(\Gamma, \mathcal{E}_N)_{(p)} = 0$ which implies from (4.18) that $H^{-1}(\Gamma, \mathcal{P}_S)_{(p)} = 0$. $\square$

Corollary . *If $L = \mathbb{Q}$ and $m_3' \geq 1$ then p divides $|Cl_N^\Gamma|$.*

Proof. This corollory follows from equation (5.1) and the fact that

$$H^0(\Gamma, Cl_N)_{(p)} = \frac{Cl_{N(p)}^{\Gamma}}{(\sum_{\gamma\in\Gamma}\gamma)Cl_{N(p)}}. \quad \square$$

CHAPTER 6

Torsion-free units of metacyclic extensions.

Introduction.

We now use the invariants we have found for lattices of pq-metacyclic groups to find the genus of the units in a metacyclic extension in certain cases.

Firstly we give the characters of the units and then we use these in sections 6.2 and 6.3 to find the possibilities for the units in two cases:

- when N is a totally real, metacyclic extension of $\mathbb{Q}$,
- when N is a complex, dihedral extension of a real field L,

and give their cohomologies.

Then we look at the case when the p-part of the class group is fixed under C_p. to give a relationship between the ramified primes and genus of U_N in this case.

Finally we study the dihedral case, i.e. when $q = 2$.

6.1. The character of U_N.

Let N be a pq-metacyclic extension of L and U_N be the torsion-free units of N. Let S_∞ be the set of infinite primes of N, then

$$U_N \otimes \mathbb{Q} \cong \Delta S_\infty \otimes \mathbb{Q}.$$

It is clear that

$$\text{character of } U_N = \text{character of } \Delta S_\infty = \text{character of } \mathbb{Z}S_\infty - \chi^+.$$

Let $d-1$ be the $\mathbb{Z}$-rank of the units in L. When N is a complex extension of a real field L then $\mathbb{Z}S_\infty \cong V^d$ and the character of U_N is

$$(d-1)\chi^+ + d\chi.$$

When N is totally real, then d is the degree of L over $\mathbb{Q}$, $\mathbb{Z}S_\infty \cong (\mathbb{Z}\Gamma)^d \cong Y^d_{T^{\max}}$ where $T^{\max} = \{0, 1, \dots, q-1\}$ and the character of U_N is

$$(d-1)\chi^+ + d\chi^- + qd\chi.$$

6.2. Torsion-free units of a totally real, metacyclic extension of $\mathbb{Q}$.

Now assume that $L = \mathbb{Q}$, i.e. $d = 1$ and N is a pq-metacyclic extension of $\mathbb{Q}$. When N is totally real, $char(U_N) = \chi^- + q\chi$.

Based on the characters the possible genera of U_N are

$$U_N \vee \left(\bigoplus_{i=0}^{q-1} P_i^{(a_i)}\right) \oplus X_T, \tag{6.1}$$

where $a_i \in \mathbb{N}$, $|T| + a_0 + \cdots + a_{q-1} = q$ and if $T = \emptyset$ then $X_T = \mathbb{S}$. The p-part of the cohomology of U_N determines its genus. Let the decomposition of U_N be as above, then

$$H^n(\Gamma, U_N)_{(p)} \cong \begin{cases} \mathbb{F}_p^{a_m} & n \equiv 2m-1 \mod (2q), \\ \mathbb{F}_p & n \equiv 2m \mod (2q), m+1 \notin T, m \neq 0, 0 \leq m \leq q-1, \\ 0 & \text{otherwise.} \end{cases} \tag{6.2}$$

Note that $H^0(\Gamma, U_N) = 0$ in all cases.

$$H^n(\Gamma, U_N)_{(q)} \cong \begin{cases} 0 & n \text{ even}, \\ \mathbb{F}_q & n \text{ odd}. \end{cases} \tag{6.3}$$

The fact that the q-parts of the cohomology are identical also follows from the following lemma.

Lemma 6.1. *([Mc], p.354, corollary 10.3) Let G be a finite group. If H is a normal subgroup of G such that $\gcd(|H|, [G : H]) = 1$ then for each G-module A and each $n \geq 1$ there is a split exact sequence*

$$0 \to H^n(G/H, A^H) \to H^n(G, A) \to H^n(H, A)^G \to 0,$$

which thus gives an isomorphism

$$H^n(G, A) \cong H^n(G/H, A^H) \oplus H^n(H, A)^G. \quad \square$$

So $H^n(\Gamma, U_N)_{(q)} \cong H^n(C_q, U_N^{C_p})$ and when $L = \mathbb{Q}$ we have $U_N^{C_p} \vee \mathbb{S}$ for all genera of U_N.

Proposition 6.2. *Let N be a real, metacyclic extension of $\mathbb{Q}$ of degree pq. Then the maximum number of genera for U_N is*

$$\sum_{n=1}^{q} \binom{q-1}{q-n} \binom{q+n-1}{q-1} = \gamma.$$

Proof. Let U_N be as in equation (6.1). Suppose $|T| = q - n$. The number of ways of choosing T is $\binom{q-1}{q-n}$.

Ways of choosing the a_i are equivalent to writing a_0 O's and then an X followed by a_1 O's and an X, etc. The total number of X's and O's is $q + n - 1$. So the number of ways of choosing the a_i corresponds to the positions of the $q - 1$ X's, which gives $\binom{q+n-1}{q-1}$.

Summing from $n = 1$ to q gives the total number of possible genera. $\square$

Note 1. γ could also be thought of as the coefficient of x^q in $\frac{(1+x)^{q-1}}{(1-x)^q}$.

Note 2. In the case when $pq = 6$ this maximum is attained. (There is an example of each in Chapter 9, section 9.1).

6.3. Torsion-free units of a complex, metacyclic extension

Let N be a complex, dihedral extension of a real field L and let the rank of the units in L be $d-1$. Then we have already shown that the character of $U_N = (d-1)\chi^+ + d\chi$. Thus the possible genera of U_N are

$$U_N \vee P_0^{(a_0)} \oplus P_1^{(a_1)} \oplus V^{d-a} \oplus \mathbb{Z}^{a-1}, \tag{6.4}$$

where $a_i \in \mathbb{N}, 1 \leq a = a_0 + a_1 \leq d$.

The cohomology of U_N is thus

$$H^n(\Gamma, U_N)_{(p)} \cong \begin{cases} \mathbb{F}_p^{a_i} & n \equiv 2i-1 \mod (2q), \\ \mathbb{F}_p^{a-1} & n \equiv 0 \mod (2q), \\ 0 & \text{otherwise.} \end{cases} \tag{6.5}$$

$$H^n(\Gamma, U_N)_{(q)} \cong \begin{cases} \mathbb{F}_q^{d-1} & n \text{ even}, \\ 0 & n \text{ odd}. \end{cases}$$

6.4. Torsion-free units when the p-part of the class group is fixed under the action of C_p.

6.4.1. Cohomology with groups fixed under the action of C_p.

Let Γ be a pq-metacyclic group and recall that C_p is a p-Sylow subgroup of Γ generated by σ.

Lemma 6.3. *Let $\mathcal{M}$ be a C_q-module of order a power of p and fixed under the action of C_p, then $\mathcal{M}$ is a product of $\mathbb{Z}$-cyclic C_q-modules. (In particular, if $\mathcal{M}$ is $\mathbb{Z}\Gamma$-module with p-primary part fixed under the actions of C_q then the p-part is a product of $\mathbb{Z}$-cyclic $\mathbb{Z}\Gamma$-modules.)*

Proof. $\mathcal{M}$ is an abelian $\mathbb{Z}_p\mathcal{C}_q$-module. Since $q|p-1$, $\mathbb{Z}_p$ contains all the qth roots of unity and $1/q$, so $\mathbb{Z}_p\mathcal{C}_q$ contains a full set of idempotents, e_χ, corresponding to the 1-dimensional representations, χ, of C_q over $\bar{\mathbb{Q}}_p$ so

$$\mathbb{Z}_p\mathcal{C}_q \cong \bigoplus_\chi \mathbb{Z}_p e_\chi.$$

All $\mathbb{Z}_p$ (and therefore all $\mathbb{Z}_p e_\chi$) modules are sums of cyclic modules. Thus $\mathcal{M}e_\chi$ is a sum of cyclic (hence $\mathbb{Z}$-cyclic) $\mathbb{Z}_p e_\chi$ modules. Hence, since the action of $\mathbb{Z}_p\mathcal{C}_q$ factors through the projection of $\mathbb{Z}_p\mathcal{C}_q$ on $\mathbb{Z}_p e_\chi$ it is a sum of $\mathbb{Z}$-cyclic $\mathbb{Z}_p\mathcal{C}_q$-modules. $\square$

Theorem 6.4. *Let T be a finite module and let the p-primary part of T be abelian and fixed under the action of C_p then*

$$H^{2n}(\Gamma, T)_{(p)} \cong H^{2n-1}(\Gamma, T)_{(p)}. \tag{6.6}$$

Proof. The p-primary part of T can be written (by lemma 6.3) as

$$T_{(p)} \cong C_1 \oplus C_2 \oplus \cdots \oplus C_s,$$

where the C_i are $\mathbb{Z}$-cyclic Γ-modules. Then $H^n(\Gamma, T)_{(p)} \cong H^n(\Gamma, C_1) \oplus \cdots \oplus H^n(\Gamma, C_s)$. Therefore without loss of generality we can assume that T is a $\mathbb{Z}$-cyclic Γ-module of order a power of p. Let $|T| = p^m$ for some positive integer m, and use induction on m.

When $m = 1$, $T \cong \mathbb{F}_p{}^{(i)}$ for some $0 \le i \le q-1$ (see section 2.2.2 for a definition of $\mathbb{F}_p^{(i)}$) and

$$H^n(\Gamma, \mathbb{F}_p{}^{(i)}) \cong \begin{cases} \mathbb{F}_p & \text{if } n \equiv 2i-1, 2i \mod (2q), \\ 0 & \text{otherwise.} \end{cases}$$

So the proposition is true when $m = 1$.

Now assume true for $m = k$. Let $|T| = p^{k+1}$ and let G be a submodule of T of order p. Then G and $T/G = H$ are cyclic p-groups with order less than or equal to p^k. Also $G \cong \mathbb{F}_p{}^{(i)}$ for some $0 \le i \le q-1$.

Take the cohomology of the short exact sequence $G \xrightarrow{g} T \xrightarrow{h} H$ by the group $\mathcal{C}_p \subset \Gamma$ to get

$$\cdots \to H^n(\mathcal{C}_p, G) \xrightarrow{g_n^*} H^n(\mathcal{C}_p, T) \xrightarrow{h_n^*} H^n(\mathcal{C}_p, H) \xrightarrow{\pi_n^*} H^{n+1}(\mathcal{C}_p, G) \to \dots. \qquad (6.7)$$

Claim: Let $\mathcal{C}$ be a $\mathbb{Z}$-cyclic Γ-module of order a power of p, on which $\mathcal{C}_p$ acts trivially, then $|H^n(\mathcal{C}_p, \mathcal{C})| = p$. Proof: From [Br], p148, theorem (8.1) we know that the fixed part of $\mathcal{C}$ under $\mathcal{C}_p$ must be non-trivial, i.e. $\mathcal{C}^{\mathcal{C}_p} \neq \{0\}$. So $H^0(\mathcal{C}_p, \mathcal{C}) \cong \mathcal{C}^{\mathcal{C}_p}/p\mathcal{C}^{\mathcal{C}_p}$. Thus the results follows using the Herbrand quotient and the periodicity of cyclic cohomology.

If the groups in the exact sequence (6.7) are all of prime order p then the maps are alternating isomorphisms and zero maps. Clearly there are two positions which we could place these in the exact sequence (6.7) corresponding to whether n is odd or even in the sequence below

$$\dots \xrightarrow{\sim} H^n(\mathcal{C}_p, G) \xrightarrow{0} H^n(\mathcal{C}_p, T) \xrightarrow{\sim} H^n(\mathcal{C}_p, H) \xrightarrow{0} H^{n+1}(\mathcal{C}_p, G) \xrightarrow{\sim} \dots. \qquad (6.8)$$

We shall now show that n must be even by considering the map

$$H^0(\mathcal{C}_p, G) \to H^0(\mathcal{C}_p, T), \qquad (6.9)$$

and showing this is a zero map.

Firstly, $H^0(\mathcal{C}_p, G) \cong G/pG = G$. Thus the map (6.9) becomes

$$G \to T^{\mathcal{C}_p}/pT^{\mathcal{C}_p}, \qquad (6.10)$$

where G maps into $T^{\mathcal{C}_p} = T$ by inclusion. If $T = \langle t \rangle$ then t^{p^k} is a generator of G. Either $G \subset pT^{\mathcal{C}_p}$ or $T^{\mathcal{C}_p} = G$ which is the case we have already proved.

Replacing $\mathcal{C}_p$ by Γ in (6.8) gives another exact sequence by theorem 2.2 (ii) and because $\mathcal{C}_p$ is a normal p-Sylow subgroup of Γ.

Let n be an even number. We have the following sequence of maps

$$H^n(\Gamma,T) \overset{h_n^*}{\to} H^n(\Gamma,H) \cong H^{n-1}(\Gamma,H) \overset{\pi_{n-1}^*}{\to}$$

$$H^n(\Gamma,G) \cong H^{n-1}(\Gamma,G) \overset{g_{n-1}^*}{\to} H^{n-1}(\Gamma,T).$$

All these maps are isomorphisms and we have proved the theorem in the case where $|H^n(C_p,C)| = p$ for all n. $\square$

Remark. For example theorem 6.4 will be true of the class group when $p^q \nmid h_N$.

Corollary . *Let N be a metacyclic extension of order pq over $\mathbb{Q}$ and let the p-part of Cl_N be a direct sum of $\mathbb{Z}$-cyclic Γ-modules fixed under the action of C_p. Let m_3' primes in $\mathbb{Q}$ have decomposition group C_p then*

$$p^{m_3'} = |Cl_N^\Gamma|_{(p)}.$$

Proof. From theorem 6.4 $|H^0(\Gamma, Cl_N)|_{(p)} \cong |H^{-1}(\Gamma, Cl_N)|_{(p)}$. Substituting this into equation (5.1) of theorem 5.5 gives the result. $\square$

6.4.2. Torsion-free units when no primes have decomposition group C_p.

Theorem 6.5. *Let N be a totally real, metacyclic extension of $\mathbb{Q}$ with p-part of the class group a product of $\mathbb{Z}$-cyclic Γ-modules fixed under C_p (for example, this occurs when $p^2 \nmid h_n$) and no ramified primes have decomposition group C_p. Let $|H^{2n-2}(\Gamma, Cl_N)|_{(p)} = p^{\mu_n}$ then*

$$m_4 = 0 \implies U_N \vee X_T \oplus P_2 \oplus (\bigoplus_{i=0}^{q-1} P_i^{\mu_i'}), \quad i+1 \in T \Leftrightarrow \mu_i' = 0,$$

$$m_4 = 1 \implies U_N \vee X_T \oplus P_1 \oplus (\bigoplus_{i=0}^{q-1} P_i^{\mu_i}), \quad i+1 \in T \Leftrightarrow \mu_i = 0,$$

$$m_4 = 2 \implies U_N \vee X_T \oplus P_1 \oplus P_1 \oplus (\bigoplus_{i=0}^{q-1} P_i^{\mu_i}), \quad i+1 \in T \Leftrightarrow \mu_i = 0,$$

In the first two cases $|T|+\mu_0+\cdots+\mu_{q-1} = q-1$. *In the third case* $|T|+\mu_0+\cdots+\mu_{q-1} = q-2$.

There are two possibilities for U_N *when* $m_4 = 0$ *because* $\mu_i' = \mu_i$ *for* $i \neq 2$, *and* $\mu_2' = \mu_2$ *or* $\mu_2 - 1$.

Let N *be a complex, dihedral extension of a real field* L, *then*

$$\begin{aligned} m_4 = 0 \quad &\Longrightarrow \quad U_N \vee P_0 \oplus \mathbb{Z}^{\mu_1} \oplus V^{d-\mu_1-1} \\ m_4 \geq 1 \quad &\Longrightarrow \quad U_N \vee P_0^{\mu_1} \oplus P_1^{1+\mu_1} \oplus V^{d-\mu_1-1} \oplus \mathbb{Z}^{\mu_1} \end{aligned}$$

Proof. We have shown in the previous sections that the only remaining invariant needed to determine the genus of U_N in these cases is the p-cohomology of U_N, i.e. $H^n(\Gamma, U_N)_{(p)}$.

We know that m_3', the number of ramified primes with decomposition group $\mathcal{C}_p$ is zero. We can choose a set of primes S such that $m_3 = 0$, i.e. no primes in S have decomposition group $\mathcal{C}_p$ by lemma 4.7.

Note that

$$\begin{aligned} m_3' = 0 &\Longrightarrow |Cl_N^\Gamma|_{(p)} = 0, \qquad \text{by the corollary to theorem' 6.4,} \\ &\Longrightarrow H^0(\Gamma, Cl_N)_{(p)} = 0, \\ &\Longrightarrow H^{-1}(\Gamma, Cl_N)_{(p)} = 0, \text{ by theorem 6.4.} \end{aligned}$$

Case A. $m_4 = 0$ (no non-split prime ideals in S)
From the exact sequences (4.13) and (4.14) it is clear that

$$H^n(\Gamma, \mathcal{P}_S)_{(p)} \cong H^{n-1}(\Gamma, Cl_N)_{(p)}. \tag{6.11}$$

From the exact sequence (4.16) and (4.17)

$$H^n(\Gamma, U_N)_{(p)} \cong H^{n-1}(\Gamma, \mathcal{P}_S)_{(p)} \text{ for } n \not\equiv 3, 4 \mod (2q).$$

Combining the last two equations gives

$$H^n(\Gamma, U_N)_{(p)} \cong H^{n-2}(\Gamma, Cl_N)_{(p)} \text{ for } n \not\equiv 3, 4 \mod (2q).$$

and thus $H^{2n}(\Gamma, U_N)_{(p)} \cong H^{2n-1}(\Gamma, U_N)_{(p)}$ for $n \not\equiv 2$.

Substituting for $H^n(\Gamma, \mathcal{P}_S)_{(p)}$ using equation (6.11) in exact sequence (4.17) gives

$$0 \to H^1(\Gamma, Cl_N)_{(p)} \to H^3(\Gamma, U_N)_{(p)} \to \mathbb{F}_p \xrightarrow{f} H^2(\Gamma, Cl_N)_{(p)} \to H^4(\Gamma, U_N)_{(p)} \to 0.$$

In the real case this gives two possibilities for the cohomology depending on whether f is zero or injective. In the non-dihedral complex case $H^4(\Gamma, U_N) = 0$ and so there is only one possibility for $H^3(\Gamma, U_N)_{(p)}$, since $H^1(\Gamma, Cl_N)_{(p)} \cong H^2(\Gamma, Cl_N)_{(p)}$ this must be $\mathbb{F}_p$.

Thus we have found the cohomology of U_N when $m_4 = 0$.

Case B. $m_4 \geq 1$ (at least one prime does not split)
From the exact sequence (4.14)

$$H^n(\Gamma, \mathcal{P}_S)_{(p)} \cong H^{n-1}(\Gamma, Cl_N)_{(p)} \text{ for } n \not\equiv 0, 1 \mod (q).$$

Since $H^0(\Gamma, Cl_N) = 0$ we get the following from exact sequence (4.13)

$$H^1(\Gamma, \mathcal{P}_S)_{(p)} = 0$$

and

$$H^0(\Gamma, \mathcal{P}_S)_{(p)} \cong \mathbb{F}_p^{m_4} \oplus H^{-1}(\Gamma, Cl_N)_{(p)}.$$

Substituting the above into exact sequence (4.18) gives

$$H^2(\Gamma, U_N)_{(p)} \cong \mathbb{F}_p^{m_4 - 1}$$

and

$$H^3(\Gamma, U_N)_{(p)} = 0.$$

Substituting into exact sequence (4.19) at $n = 0$ gives

$$H^0(\Gamma, U_N)_{(p)} \cong H^{-2}(\Gamma, Cl_N)_{(p)}$$

and

$$H^1(\Gamma, U_N)_{(p)} \cong \mathbb{F}_p^{m_4} \oplus H^{-1}(\Gamma, Cl_N)_{(p)}. \equiv \mathbb{F}_p^{m_4}$$

Finally, looking at exact sequence (4.19) for all $n \not\equiv 0, 1 \mod (2q)$ gives

$$H^n(\Gamma, U_N)_{(p)} \cong H^{n-2}(\Gamma, Cl_N)_{(p)} \text{ for } n \not\equiv 1, 2, 3 \mod (2q).$$

Thus we have the p-cohomology for U_N when $m_4 \geq 1$.

Now the torsion-free lattices in the theorem have the correct cohomology and characters. Thus by theorem 2.6, they lie in the genus of U_N. This completes the proof of theorem 6.5. □

6.4.3. Torsion-free units when the p-part of the class group is trivial.

In this section assume that $p \nmid h_N$. So $H^n(\Omega, Cl_N)_{(p)} = 0$ for all n, implying by the exact sequence (2.13), $H^n(\Omega, \mathcal{P}_S)_{(p)} \cong H^n(\Omega, \mathbb{Z}S_f)_{(p)}$ for all subgroups $\Omega \subset \Gamma$. In theorem 6.6 we show that when N is real m_4, the number of ramified, non-split primes determines the p-part of the cohomology of U_N, and, hence, when N is a metacyclic extension of $\mathbb{Q}$, determines the genus of U_N. We find that when N is a complex metacyclic extension of L then m_4 determines U_N exactly.

From theorem 5.5, if $p \nmid h_N$ then $m_3' = 0$, i.e. no ramified primes have decomposition group $\mathcal{C}_p$. So the following theorem is can be obtained as a corollary to theorem 6.5.

Theorem 6.6. *(i) Let N be a totally real, metacyclic extension of L of degree pq with $p \nmid h_N$, then m_4, the number of non-split, ramified primes determines the p-part of the cohomology of U_N. (Thus, the additional information needed to determine the genus is the q-part of the cohomology which is given by $H^n(\mathcal{C}_q, U_N^{\mathcal{C}_p}) = H^n(\mathcal{C}_q, U_K)$.)*

If N is a metacyclic extension of $\mathbb{Q}$ then m_4 determines the genus of the torsion-free units and $m_4 \leq 2$.

$$m_4 = 0 \implies U_N \vee X_T \oplus P_2, \quad T = \{2, 3, \ldots, q\},$$
$$m_4 = 1 \implies U_N \vee X_T \oplus P_1, \quad T = \{2, 3, \ldots, q\},$$
$$m_4 = 2 \implies U_N \vee X_T \oplus P_1 \oplus P_1, \quad T = \{3, 4, \ldots, q\}.$$

(ii) Let N be a complex, dihedral extension of a real field L with $p \nmid h_N$ and let $d-1$ be the $\mathbb{Z}$-rank of the units in L. Then $m_4 \leq 1$ and

$$m_4 = 0 \implies U_N \vee P_2 \oplus V^{d-1}$$
$$m_4 = 1 \implies U_N \vee P_1 \oplus V^{d-1} \quad \square$$

Corollary . *Let N be a real, metacyclic extension of $\mathbb{Q}$ of degree pm, then*

$$m_4 = 0 \implies \widehat{U_N} \cong \oplus_{t=2}^{q} \widehat{\mathbb{Z}_{t-1}^{\Gamma}} \oplus \widehat{P_2},$$
$$m_4 = 1 \implies \widehat{U_N} \cong \oplus_{t=2}^{q} \widehat{\mathbb{Z}_{t-1}^{\Gamma}} \oplus \widehat{P_1},$$
$$m_4 = 2 \implies \widehat{U_N} \cong \oplus_{t=3}^{q} \widehat{\mathbb{Z}_{t-1}^{\Gamma}} \oplus \widehat{P_1} \oplus \widehat{P_1}.$$

Proof. Using proposition 2.5 we could replace q by a non-prime m dividing $p-1$ and replace the units by their p-adic completions. $\square$

Note. This would also be possible for proposition 4.5 and theorem 6.5.

6.5. Torsion-free units of dihedral extensions.

Let N be a dihedral extension of L of degree $2p$ with Galois group Γ. Then there are 10 indecomposable Γ-lattices as we have discussed in Chapter 1; $\mathbb{Z}, \mathbb{Z}^-, \mathbb{Z}C_q, R, P, V, X, Y_0, Y_1$ and Y_2.

When N is real, for a general field L it can be difficult to say anything about the structure of the units, but in section 6.5.1 looking at the simplest case (when $m_3 = m_4 = 0$ and the class group is trivial) we can get some results. (See proposition 6.7.)

In the following two sections we consider the case $L = \mathbb{Q}$ when N is real and complex.

Finally, when N is a complex, dihedral extension of a quadratic field the results are very similar to those when N is a real, dihedral extension of $\mathbb{Q}$.

6.5.1. $\mathbf{U_N}$ when $\mathbf{m_3 = m_4 = 0}$.

Proposition 6.7. *Let N be a totally real extension of L, L a Galois extension of degree d over $\mathbb{Q}$, $m_3 = m_4 = 0$ and $h_N = 1$ then there are at most $5 - \log_2[(h_L)_{(2)}]$ possibilities for the genus of U_N as a Γ-module, namely*

$$U_N \vee X^{\alpha+1} \oplus R \oplus V^{\alpha} \oplus {Y_2}^{d-1-\alpha},$$

for $m_2' - \log_2[(h_L)_{(2)}] - 4 \leq \alpha \leq m_2'$.

Remark. It is clear from the characters and cohomology of Y_2 that $\mathbb{Z}\Gamma \vee Y_2$. So when m_2' is large U_N is not a product of $X \oplus R$ and a free module ($U_N \vee X \oplus R$ when $d = 1$.)

Proof. The class group of N is trivial implies that

$$\mathbb{Z}S_f \cong \mathcal{P}_S.$$

From the exact sequences (4.16) and (4.17) we know

$$H^1(\Gamma, U_N)_{(p)} = H^2(\Gamma, U_N)_{(p)} = H^0(\Gamma, U_N)_{(p)} = 0$$

and

$$H^{-1}(\Gamma, U_N)_{(p)} \cong \mathbb{F}_p.$$

So $\mathbb{Z}^-, P, \mathbb{Z}H, Y_0$ and Y_1 are not direct summands of U_N, and exactly one direct summand is in the genus of R.

$H^0(\Gamma, U_N)_{(2)} \subset H^0(\Gamma, U_S)_{(2)} \subset \mathbb{F}_2{}^{m_2}$. Let $H^0(\Gamma, U_N)_{(2)} \cong \mathbb{F}_2{}^{\alpha}$, then this and the characters give the result.

If $H^0(\Gamma, U_N)_{(2)} = \oplus_\alpha \mathbb{F}_2$ then using theorem 2.6

$$U_N \vee X^{\alpha+1} \oplus R \oplus V^{\alpha} \oplus Y_2{}^{d-1-\alpha},$$

All that remains to be proved is that

$$m_2 - \log_2(h_L)_{(2)} - 4 \leq \alpha \leq m_2.$$

Sequence (4.17) and the fact that $H^0(\Gamma, \mathbb{Z}S_f)_{(2)} \cong H^0(\Gamma, \mathcal{P}_S)_{(2)} = 0$ give

$$H^0(\Gamma, U_N)_{(2)} \subset H^0(\Gamma, U_S)_{(2)}.$$

Now, $H^0(\Gamma, \mathcal{E}_S)_{(2)} \cong \mathbb{F}_2^{m_2-1}$ and $H^1(\Gamma, \mu)_{(2)} \cong \mathbb{F}_2$ imply that the largest $H^0(\Gamma, U_S)_{(2)}$ can be (and thus an upper bound for $H^0(\Gamma, U_N)_{(2)}$) is $\mathbb{F}_2^{m_2}$. Since we can choose $m_2 = m_2'$ we have $\alpha \leq m_2'$.

Now, equation (5.8) still applies when $m_3 + m_4 = 0$, take the 2-part with $\Omega = \Gamma$, then

$$|H^1(\Gamma, \mathcal{P}_S)|_{(2)} = \frac{|Cl_N|_{(2)} \times |H^1(\Gamma, \mathcal{E}_N)|_{(2)}}{|Cl_L|_{(2)} \times [\mathbb{Z}S_f^{\Gamma} : \mathbb{Z}S_{f,L}]_{(2)}},$$

$$1 = \frac{1 \times |H^1(\Gamma, \mathcal{E}_N)|_{(2)}}{(h_L)_{(2)} \times 2^{m_2'}},$$

implying

$$|H^1(\Gamma, \mathcal{E}_N)|_{(2)} = (h_L)_{(2)} \times 2^{m_2'}.$$

Sequence 2.10 with $H^{-1}(\Gamma, \mathcal{P}_S)_{(2)} = H^1(\Gamma, \mathcal{P}_S)_{(2)} = 0$ and $H^0(\Gamma, \mathcal{P}_S)_{(2)} = \mathbb{F}_2^{m_2}$ gives

$$0 \to H^0(\Gamma, U_N)_{(2)} \to H^0(\Gamma, U_S)_{(2)} \to \mathbb{F}_2^{m_2} \to H^1(\Gamma, U_N)_{(2)} \to H^1(\Gamma, U_S)_{(2)} \to 0.$$

So, the smallest possible value of $|H^0(\Gamma, U_N)|_{(2)}$ occurs when

$|H^0(\Gamma, U_S)|_{(2)}$ is smallest and

$$|H^0(\Gamma, U_S)|_{(2)} \geq 2^{m_2-2},$$

$|H^1(\Gamma, U_N)|_{(2)}$ is smallest and

$$|H^1(\Gamma, U_N)|_{(2)} \geq 2^{m_2+log_2(h_L)_{(2)}-1},$$

$|H^1(\Gamma, U_S)|_{(2)}$ is largest and

$$|H^1(\Gamma, U_S)|_{(2)} \leq 2,$$

Combining these gives

$$|H^0(\Gamma, U_N)|_{(2)} \geq 2^{m_2-2+m_2'+log_2(h_L)_{(2)}-1}/2^{m_2+1} = 2^{m_2'+log_2(h_L)_{(2)}-4}.$$

Hence $\alpha \geq m_2' + log_2(h_L)_{(2)} - 4$ as required. □

6.5.2. Totally real dihedral extensions of $\mathbb{Q}$.

Let $L = \mathbb{Q}$, then based on the characters there are five possibilities for U_N. The possible structures for U_N as a direct sum of indecomposable modules are $\mathbb{Z}^- \oplus R \oplus R$, $\mathbb{Z}^- \oplus R \oplus P$, $\mathbb{Z}^- \oplus P \oplus P$, $X \oplus R$, and $X \oplus P$, and each of these represents a distinct genus.

Proposition 6.8. *Let N be a totally real, pq-metacyclic extension of $\mathbb{Q}$.*
Case A. *If $N/\mathbb{Q}$ has no decomposition groups Γ or C_p, i.e. $m_3 = m_4 = 0$, then*

$$U_N \vee \mathbb{Z}^- \oplus R \oplus R \text{ or } X \oplus R.$$

Case B. *If $m_3 + m_4 \geq 1$ then given the cohomology of the class group and m_4 there are up to three possibilities for the genus of U_N:*

$m_4 - \mu_3 + \mu_4$	$H^1(\Gamma, \mathcal{P}_S)_{(p)}$	*Genus of* U_N
2	0	$\mathbb{Z}^- \oplus P \oplus P$
1	0	$X \oplus P$
	0	$\mathbb{Z}^- \oplus R \oplus P$
	$\mathbb{F}_p$	$\mathbb{Z}^- \oplus P \oplus P$
0	0	$X \oplus R$
	0	$\mathbb{Z}^- \oplus R \oplus R$
	$\mathbb{F}_p$	$\mathbb{Z}^- \oplus R \oplus P$
-1	$\mathbb{F}_p$	$\mathbb{Z}^- \oplus R \oplus R$

where $|H^n(\Gamma, Cl_N)|_{(p)} = p^{\mu_n}$.

Proof. If we write $p^{\nu_n} = |H^n(\Gamma, U_N)|_{(p)}$, then any two of ν_1, ν_2 and ν_3 determine U_N.

U_∞	ν_1	ν_2	ν_3	ν_4
$\mathbb{Z}^- \oplus R \oplus R$	0	1	2	0
$\mathbb{Z}^- \oplus R \oplus P$	1	1	1	0
$\mathbb{Z}^- \oplus P \oplus P$	2	1	0	0
$X \oplus R$	0	0	1	0
$X \oplus P$	1	0	0	0

Case A. If $m_3 = m_4 = 0$ then

$$|H^1(\Gamma, \mathcal{P}_S)|_{(p)} \cong |H^0(\Gamma, Cl_N)|_{(p)} = \frac{|Cl_N^\Gamma|_{(p)}}{[(\sum_{\gamma\in\Gamma}\gamma)Cl_N]_{(p)}} \tag{6.12}$$

(5.8) is true when $m_3 = m_4 = 0$ and in this case $[\mathbb{Z}S_f{}^\Gamma : \mathbb{Z}\hat{S}_f]_{(p)} = 1$. Because $L = \mathbb{Q}$, $Cl_L = 0$.

Equating the p-parts of (5.8) and (6.12) we have

$$|H^1(\Gamma, U_N)|_{(p)} = \frac{1}{[(\sum_{\gamma\in\Gamma}\gamma)Cl_N]_{(p)}}. \tag{6.13}$$

Implying that $|H^1(\Gamma, U_N)|_{(p)} = 1$ and therefore

$$U_N \vee \mathbb{Z}^- \oplus R \oplus R \text{ or } X \oplus R.$$

Case B. If $m_3 + m_4 \geq 1$ then $H^0(\Gamma, U_N) = 0$ implies $H^{-1}(\Gamma, \mathcal{P}_S) = 0$ (from (4.18)).

Using the exact sequences (4.18) and (4.13) it is seen that

$$|H^1(\Gamma, U_N)|_{(p)} = |H^1(\Gamma, \mathcal{P}_S)|_{(p)} \times p^{m_4+\mu_3-\mu_4}, \tag{6.14}$$

where $|H^n(\Gamma, Cl_N)|_{(p)} = p^{\mu_n}$ and we know that $H^1(\Gamma, \mathcal{P}_S)_{(p)} \subset H^2(\Gamma, U_N)_{(p)}$ from (4.15).

So, given the class group and m_4 there are up to three possibilities for the genus of U_N. □

Corollary . *When the p-part of Cl_N is abelian and fixed under the action of C_p then by proposition 6.4 we know that $\mu_3 = \mu_4$. So m_4 is at most 2.* □

6.5.3. Complex dihedral extensions of $\mathbb{Q}$.

Now there are only two possibilities for U_N, namely R or P. In a similar way to subsection 6.5.2 we get:

Proposition 6.9. *Let N be a complex, pq-metacyclic extension of $\mathbb{Q}$.*
Case A. *When $m_3 = m_4 = 0$ then*

$$U_N \vee R.$$

Case B. *When $m_3 + m_4 \geq 1$ then*

$$m_4 = -\mu_1 + \mu_2 \text{ implies } U_N \vee R,$$

$$m_4 = -\mu_1 + \mu_2 + 1 \text{ implies } U_N \vee P. \quad \square$$

Now applying proposition 6.4.

Corollary . *If the p-part of Cl_N is abelian and fixed under the action of C_p then m_4 determines the genus of U_N.*

$$m_4 = 0 \textit{ implies } U_N \vee R,$$

$$m_4 = 1 \textit{ implies } U_N \vee P. \quad \square$$

6.5.4. Complex, dihedral extensions of quadratic fields.

When L is a totally real quadratic extension of $\mathbb{Q}$ and N is a complex extension of L we get results parallel to those of the totally real case. The character of U_N is $\chi^+ + 2(\chi_1 + \ldots \chi_r)$ and this gives five possibilities for U_N, which are $\mathbb{Z} \oplus R \oplus R, \mathbb{Z} \oplus R \oplus P, \mathbb{Z} \oplus P \oplus P, V \oplus R$ and $V \oplus P$.

When $m_3 = m_4 = 0$ we find $U_N \vee \mathbb{Z} \oplus R \oplus R$ or $V \oplus R$.

When $m_3 + m_4 \geq 1$ we can find possibilities for the genus of U_N given the class group and m_4.

m_4	$H^1(\Gamma, \mathcal{P}_S)_{(p)}$	U_N
$3 - \mu_1 + \mu_2$	0	$\mathbb{Z} \oplus R \oplus R$
$2 - \mu_1 + \mu_2$	0	$V \oplus R$
	0	$\mathbb{Z} \oplus R \oplus P$
	$\mathbb{F}_p$	$\mathbb{Z} \oplus R \oplus R$
$1 - \mu_1 + \mu_2$	0	$V \oplus P$
	0	$\mathbb{Z} \oplus R \oplus P$
	$\mathbb{F}_p$	$\mathbb{Z} \oplus P \oplus P$
$-\mu_1 + \mu_2$	$\mathbb{F}_p$	$\mathbb{Z} \oplus P \oplus P$

When Cl_N is a product of $\mathbb{Z}$-cyclic Γ- modules invariant under the action of C_p then $\mu_1 = \mu_2$.

CHAPTER 7

Unit invariants in the factorizability defect group.

Introduction.

If we try to study the torsion-free units of a pq-metacyclic extension of $\mathbb{Q}$ in $\mathcal{G}_0(\mathbb{Z}\Gamma)$, the Grothendieck group of Γ-modules with respect to exact sequences, we find that $[U_N] = [\Delta S_\infty]$ for all torsion-free units U_N. We need to work in a larger group to distinguish between units of different genera.

In section 7.1 the factorizability defect Grothendieck group is defined and it is shown that in this group $[P_i] \neq [P_j]$ when $i \not\equiv j \mod (q)$. Thus we can determine between the genus of some Γ-lattices working in this group. Unfortunately it is also shown that $[X_T] = [X_{T\setminus i}] + [P_{i-1}]$ and thus it will not always be possible to distinguish between all the possible cases for the genus of the units.

We will then find some equations including the units in the factorizability defect group and use these to get some results on the genus of the units.

In this section $\mathcal{M}_p$ means p-adic completion of $\mathcal{M}$ (although in other chapters we have used $\widehat{\mathcal{M}}$).

7.1. The factorizability defect Grothendieck group.

Definition. Let Γ be a finite group. From [HW1] and [HW2], define the **factorizability defect Grothendieck group,** $\mathcal{G}_0^{fd}(\mathbb{Z}\Gamma)$ generated by isomorphism classes of Γ-modules and elements of the factorizability defect group (defined below) with relations given by short exact sequences. Given a short exact sequence of Γ-modules

$$E: \quad 0 \to M' \to M \to M'' \to 0,$$

then in $\mathcal{G}_0^{fd}(\mathbb{Z}\Gamma)$ there is a relation

$$[M'] - [M] + [M''] = [fd(E)]_{fd}, \tag{7.1}$$

where $fd(E)$ is called the **factorizability defect** of the exact sequence E which is defined below and we write

$$E: \quad 0 \to M' \to M \to M'' \to 0 \qquad\qquad [fd(E)]_{fd}. \tag{7.2}$$

Let $W = \bigcup_\Omega \Gamma/\Omega$, the disjoint union over all subgroups, Ω, of Γ and let $H_\Gamma^n(-)$ be the **Hecke cohomology group** obtained from the derived functors of

$$- \otimes_{\mathbb{Z}\Gamma} \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[W], \mathbb{Z}) \text{ and } \mathrm{Hom}_{\mathbb{Z}\Gamma}(\mathbb{Z}[W], -),$$

in the same way as the Tate cohomology groups are obtained from the homology and cohomology groups (see [Ho].)

Then $fd(E) = [\mathrm{coker}(\,\alpha_\Gamma^0 : H_\Gamma^0(M) \to H_\Gamma^0(M''))] \in \mathcal{G}_0^t(\mathrm{End}_{\mathbb{Z}\Gamma}(\mathbb{Z}W))$.

We shall write $\mathrm{End}_{\mathbb{Z}\Gamma}(\mathbb{Z}W)$ as Λ.

Theorem 7.1. *Let Γ be the metacyclic group of order pq, then $[P_i] \neq [P_j]$ in the factorizability defect group $\mathcal{G}_0^{fd}(\mathbb{Z}_p\Gamma)$ whenever $i \not\equiv j \mod (q)$.*

Proof. There is a surjection, $\mathbb{Z}_p\Gamma \twoheadrightarrow \widetilde{R_p\mathcal{C}_q}$, where $\widetilde{R_p\mathcal{C}_q}$ is a twisted group ring and $\widetilde{R_p\mathcal{C}_q} \cong \coprod_{i=0}^{q-1}(P_i)_p$.

Therefore

$$\mathcal{G}_0(\widetilde{R_p\mathcal{C}_q}) \cong \mathcal{K}_0(\widetilde{R_p\mathcal{C}_q}) \cong \langle [(P_0)_p], [(P_1)_p], \ldots, [(P_{q-1})_p] \rangle.$$

If there exists a homomorphism from $\mathcal{G}_0^{fd}(\mathbb{Z}_p\Gamma)$ to $\mathcal{G}_0(\widetilde{R_p\mathcal{C}_q})$ which maps P_i to P_i, then the P_i must be distinct in $\mathcal{G}_0^{fd}(\mathbb{Z}_p\Gamma)$.

Define a functor $F : \mathrm{Mod}(\mathbb{Z}_p\Gamma) \to \mathrm{Mod}(\widetilde{\mathrm{R_p\mathcal{C}_q}})$ by $F : M \mapsto M/M^{C_p}$ for any Γ-module M, then F maps P_i to P_i. For F to induce a homomorphism from $\mathcal{G}_0^{fd}(\mathbb{Z}_p\Gamma)$

to $\mathcal{G}_0(\widetilde{R_p\mathcal{C}_q})$, it is also necessary to define F on the factorizability defects such that for any exact sequence (7.2),

$$[F(M')] - [F(M)] + [F(M'')] = [F(fd(E))] \text{ in } \mathcal{G}_0(\widetilde{R_p\mathcal{C}_q}).$$

Let Ω be a subgroup of Γ. There exists an idempotent $f_\Omega \in \mathrm{End}(\mathbb{Z}[W])$ which gives a projection from $\mathbb{Z}[W]$ onto $\mathbb{Z}[\Omega \setminus \Gamma]$, so that

$$\mathbb{Z}[W].f_\Omega \cong \mathbb{Z}[\Omega \setminus \Gamma].$$

Then $\mathrm{Hom}_{\mathbb{Z}\Gamma}(\mathbb{Z}[W], M)$ is defined to be M^W, and

$$\mathrm{Hom}_{\mathbb{Z}\Gamma}(\mathbb{Z}[W], M).f_\Omega \cong \mathrm{Hom}_{\mathbb{Z}\Gamma}(\mathbb{Z}[\Omega \setminus \Gamma], M) \cong M^\Omega.$$

$$.f_\Omega : \mathrm{Mod}(\Lambda) \to \mathrm{Mod}(\mathbb{Z}(\mathrm{N}_\Gamma(\Omega)/\Omega)),$$

where N_Γ is the normalizer. So $.f_\Omega$ induces a map $\mathcal{G}_0^t(\Lambda_p).f_\Omega$ into $\mathcal{G}_0^t(\mathbb{Z}_p[N_\Gamma(\Omega)/\Omega])$. We write $fd(E).f_\Omega$ as $fd_\Omega(E)$. Given an exact sequence (7.2) we can fix this by W. As f_Ω is an idempotent, the corresponding functor $.f_\Omega$ is exact and we get

$$\begin{array}{ccccccccc}
0 & \longrightarrow & (M')^W & \longrightarrow & (M)^W & \longrightarrow & (M'')^W & \longrightarrow & fd(E) & \longrightarrow & 0 \\
 & & \downarrow{\cdot f_\Omega} & & \downarrow{\cdot f_\Omega} & & \downarrow{\cdot f_\Omega} & & \downarrow{\cdot f_\Omega} & & \\
0 & \longrightarrow & (M')^\Omega & \longrightarrow & (M)^\Omega & \longrightarrow & (M'')^\Omega & \longrightarrow & fd_\Omega(E) & \longrightarrow & 0
\end{array}$$

Let $\overline{M^\Omega}$ be the kernel of the map $(M'')^\Omega \to fd_\Omega(E)$. Then by the snake lemma we have a diagram of short exact sequences.

$$\begin{array}{ccccc}
(M')^\Omega & \longrightarrow & (M)^\Omega & \longrightarrow & \overline{M^\Omega} \\
\downarrow & & \downarrow & & \downarrow \\
M' & \longrightarrow & M & \longrightarrow & M'' \\
\downarrow & & \downarrow & & \downarrow \\
M'/(M')^\Omega & \longrightarrow & M/(M)^\Omega & \longrightarrow & M''/\overline{M^\Omega}
\end{array}$$

Which implies

$$[M'/(M')^{\Omega}] - [M/(M)^{\Omega}] + [M''/\overline{M^{\Omega}}] = 0,$$

in $\mathcal{G}_0(\widetilde{R_p\mathcal{C}_q})$.

The short exact sequence

$$(M'')^{\Omega}/\overline{M^{\Omega}} \to M''/\overline{M^{\Omega}} \to M''/(M'')^{\Omega},$$

and the fact $fd_{\Omega}(E) \cong (M'')^{\Omega}/\overline{M^{\Omega}}$ give

$$[fd_{\Omega}(E)] - [M''/\overline{M^{\Omega}}] + [M''/(M'')^{\Omega}] = 0.$$

Thus

$$[M'/(M')^{\Omega}] - [M/(M)^{\Omega}] + [M''/(M'')^{\Omega}] = -[fd_{\Omega}(E)].$$

Let $\Omega = \mathcal{C}_p$, then $\mathcal{G}_0^t(\mathbb{Z}_p[N(\Omega)/\Omega]) \cong \mathcal{G}_0^t(\mathbb{Z}_p\mathcal{C}_q)$. If torsion modules $T, T' \in \mathcal{G}_0^t(\mathbb{Z}_p\mathcal{C}_q)$ and $T' \subset T$ then $[T] = [T'] + [T/T']$, so the generators of $\mathcal{G}_0^t(\mathbb{Z}_p\mathcal{C}_q)$ are simple modules.

Every $\mathbb{Z}_p\mathcal{C}_q$-module is a $\mathbb{F}_p\mathcal{C}_q$-module and there are q simple $\mathbb{F}_p\mathcal{C}_q$-modules, namely ${\mathbb{F}_p}^{(i)} \cong P_i/P_{i-1}$.

Let T be a defect with $\mathbb{F}_p^{(i)}$ occurring $n_i \geq 0$ times in its Jordan-Hölder decomposition. Define the functor F to first send a defect $[T] \in \mathcal{G}_0^t(\mathbb{Z}_p\Gamma)$ to $-[T] = -\sum_{i=0}^{q-1} n_i {\mathbb{F}_P}^{(i)}$ in $\mathcal{G}_0^t(\mathbb{Z}_p\mathcal{C}_q) \cong \mathcal{G}_0^t(\widetilde{R_p\mathcal{C}_q})$. The exact sequence

$$\cdots \to K_1(\widetilde{K_p\mathcal{C}_q}) \to \mathcal{G}_0^t(\widetilde{R_p\mathcal{C}_q}) \xrightarrow{\phi} K_0(\widetilde{R_p\mathcal{C}_q}) \to K_0(\widetilde{K_p\mathcal{C}_q}) \tag{7.3}$$

gives a map ϕ defined by

$$\phi : {\mathbb{F}_p}^{(i)} = [P_i/P_{i-1}] \mapsto [P_i] - [P_{i-1}],$$

which completes the homomorphism

$$\mathcal{G}_0^t(\mathbb{Z}_p\Gamma) \to K_0(\widetilde{R_p\mathcal{C}_q}) = \mathcal{G}_0(\widetilde{R_p\mathcal{C}_q}),$$

as required. Thus the P_i are distinct in the factorizability defect group. $\square$

Proposition 7.2. *In* $\mathcal{G}_0^{fd}(\mathbb{Z}\Gamma)$ ·

$$[X_{T\setminus i}] - [X_T] + [P_{i-1}] = 0 \quad \textit{for } i \neq 1. \tag{7.4}$$

Proof. It is clear from [CR1], §34E that there is a short exact sequence $X_{T\setminus i} \to X_T \to P_{i-1}$ for $i \in T \subset \{0, 2, 3, \ldots, q-1\}$ and $X_\emptyset$ defined as $\mathbb{S}$.

The defect is zero because $H^0_\Gamma(P_{i-1}) = 0$ and the cokernel of $H^0_\Gamma(X_{T\setminus i}) \to H^0_\Gamma(X_T)$ lies in there. So we have

$$0 \to X_{T\setminus i} \to X_T \to P_{i-1} \to 0 \qquad [0]_{fd} \tag{7.5}$$

which gives the required result. □

7.2. Two equations in the factorizability defect group.

Using some equations in $\mathcal{G}_0^{fd}(\mathbb{Z}\Gamma)$ from [Ho] we derive two equations, (7.9) and (7.13), which give information about the genus of U_N.

Since the P_i are distinct in $\mathcal{G}_0^{fd}(\mathbb{Z}\Gamma)$ we should be able to get some information about U_N working in this Grothendieck group. Equation (3.15) of [Ho] states

$$[\mathcal{E}_N] - [\Delta S_\infty] = \Omega_3 + [Cl_N] - [(Cl_N)^W]_{fd} + [Cl_{N^W}]_{fd} - [\,H^0_\Gamma(\Delta S_\infty)]_{fd}, \tag{7.6}$$

in $\mathcal{G}_0^{fd}(\mathbb{Z}\Gamma)$, where Ω_3 is Chinburg's invariant.

Localise equation (7.6) with respect to p to get an equation in $\mathcal{G}_0^{fd}(\mathbb{Z}_p\Gamma)$ with $\Omega_3 = 0$ because Chinburg's invariant is the difference of two locally free modules. Also $[\mathcal{E}_N] = [U_N]$ because $p \nmid |\mu_N|$. Use the functor F defined above to map this into $\mathcal{G}_0(\widetilde{R_p\mathcal{C}_q})$ giving

$$[F(U_N)] - [F(\Delta S_\infty)] = [Cl_N/(Cl_N)^{\mathcal{C}_p}] + [(Cl_N)^{\mathcal{C}_p}] - [Cl_K] + [\,H^0_{\mathcal{C}_p}(\Delta S_\infty)]. \tag{7.7}$$

where K is the subfield of N fixed by $\mathcal{C}_p$.

All modules on the right hand side of the equation are torsion modules so we pull this equation back into $\mathcal{G}_0^t(\widetilde{R_p\mathcal{C}_q})$ through ϕ. Now, $\mathcal{G}_0^t(\widetilde{R_p\mathcal{C}_q}) \cong \mathcal{G}_0^t(\mathbb{Z}_p\mathcal{C}_q)$ since the simple modules in each case are the ${\mathbb{F}_p}^{(i)}$.

Note that

$$\phi : \sum_{i=0}^{q-1} {\mathbb{F}_p}^{(i)} \mapsto \sum_{i=0}^{q-1}([P_i] - [P_{i-1}]) = 0.$$

So $\sum_{i=0}^{q-1} {\mathbb{F}_p}^{(i)}$ generates the kernel of ϕ and we may factor out by this and thus we have an equation in $\mathcal{G}_0^t(\mathbb{Z}_p\mathcal{C}_q)/\langle\sum_{i=0}^{q-1} {\mathbb{F}_p}^{(i)}\rangle$.

Write $\mathcal{G}_0^t(\mathbb{Z}_p\mathcal{C}_q)/\langle\sum_{i=0}^{q-1} {\mathbb{F}_p}^{(i)}\rangle$ as $\mathcal{G}_\Gamma$.

The short exact sequence

$$0 \to (Cl_N)^{\mathcal{C}_p} \to Cl_N \to Cl_N/(Cl_N)^{\mathcal{C}_p} \to 0, \tag{7.8}$$

gives the relationship

$$[Cl_N/(Cl_N)^{\mathcal{C}_p}] = [Cl_N] - [(Cl_N)^{\mathcal{C}_p}],$$

in $\mathcal{G}_0^t(\mathbb{Z}_p\mathcal{C}_q)$.

So finally we have the following equation in $\mathcal{G}_\Gamma$

$$\boxed{\phi^{-1}([F(U_N)] - [F(\Delta S_\infty)]) = [Cl_N] - [Cl_K] + [H^0_{\mathcal{C}_p}(\Delta S_\infty)]}. \tag{7.9}$$

Proposition 7.3. *Let N/K be a cyclic Galois extension of prime degree p. If N/K is ramified then*

$$[Cl_K] \subseteq [Cl_N].$$

meaning that if we decompose $[Cl_N]$ as a sum of simple modules, $[\mathbb{F}_p^{(i)}]$, with positive coefficients and minimal in number, they will be contained inside the same decomposition of $[Cl_K]$. (i.e. The Jordan-Hölder decomposition of Cl_K is contained inside that of Cl_k.)

Proof.

Let F be the conductor of the extension, $CF(K)$ be the F-ray class group of K and $I_F(N)$ be the fractional ideals of N not involving primes dividing F.

By class field theory, there exists an exact sequence

$$I_F(N) \xrightarrow{n} CF(K) \xrightarrow{\alpha} \mathrm{Gal(N/K)} \to 1,$$

where $n(I) = [N_{N/K}(I)]$ and α is the Artin map.

Let X be the kernel of the projection

$$r : CF(K) \to Cl_K.$$

By class field theory, since N/K is ramified, α must be non-trivial on X. Since $\mathrm{Gal(N/K)}$ has no non-trivial subgroups

$$\alpha(X) = \mathrm{Gal(N/K)}.$$

So we have a diagram:

$$\begin{tikzcd}
 & X \arrow[d] \arrow[dr, "\alpha"] & \\
I_F(N) \arrow[r, "n"] \arrow[d] \arrow[dr, "\beta"] & CF(K) \arrow[r, "\alpha"] \arrow[d, "r"] & C_p \\
Cl_N \arrow[r, "\gamma"] & Cl_K &
\end{tikzcd}$$

Choose $y \in Cl_K$. Take $z \in CF(K)$ such that $r(z) = y$, and take $x \in X$ such that $\alpha(x) = \alpha(z)$.

Then $\alpha(z/x) = 1$ and so $z/x = n(I)$ for some ideal I in N. But then

$$r(n(I)) = r(z/x) = r(z) = y.$$

So $ron = \beta$ is surjective. As β factors through Cl_N it must be true that γ is surjective.

So there is a short exact sequence

$$0 \to \mathrm{Ker}(\gamma) \to Cl_N \xrightarrow{\gamma} Cl_K \to 0,$$

and hence

$$[Cl_N] = [Cl_K] + [\mathrm{Ker}(\gamma)]. \quad \square$$

If we now turn our attention to the cohomology group of the units then these provide the extra invariants needed to distinguish between units in $\mathcal{G}_\Gamma$, because even though

$$[X_T] = [X_{T\setminus i} \oplus P_{i-1}],$$

the cohomology gives

$$[H^1_{C_p}(X_T)] = 0 \text{ and } [H^1_{C_p}(X_{T\setminus i} \oplus P_{i-1})] = \mathbb{F}_p^{(q-i)}$$

So we shall map a cohomology group of the units into $\mathcal{G}_\Gamma$.

Equation (3.5) of [Ho] says

$$[H^1_\Gamma(\mathcal{P}_S)]_{fd} = [Cl_N^W]_{fd} - [\mathfrak{J}^W_{S,N}/\mathfrak{J}_{S,N^W}]_{fd} - [Cl_{N^W}]_{fd} + [H^1_\Gamma(\mathcal{E}_N)]_{fd}, \tag{7.10}$$

where $\mathfrak{J}_{S,N}$ are the fractional ideals of N supported on the places in S_f.

And from equation (3.13) of [Ho] (using (3.7))

$$[H^0_\Gamma(\mathbb{Z}S_f)]_{fd} = [\mathfrak{J}^W_{S,N}/\mathfrak{J}_{S,N^W}]_{fd}. \tag{7.11}$$

Thus adding (7.10) to (7.11) and rearranging gives

$$[H^1_\Gamma(\mathcal{E}_N)]_{fd} = [H^1_\Gamma(\mathcal{P}_S)]_{fd} - [Cl_N^W]_{fd} + [Cl_{N^W}]_{fd} + [H^0_\Gamma(\mathbb{Z}S_f)]_{fd}, \tag{7.12}$$

which remains the same with Γ and W replaced by C_p as all the parts are factorizability defects. Also, since $p \nmid |\mu_N|$ we have $[H^1_{C_p}(\mathcal{E}_N)] = [H^1_{C_p}(U_N)]$. Thus we have the following equation in $\mathcal{G}_\Gamma$

$$\boxed{[H^1_{C_p}(U_N)] = [H^1_{C_p}(\mathcal{P}_S)] - [Cl_N^{C_p}] + [Cl_K] + [H^0_{C_p}(\mathbb{Z}S_f)]}. \tag{7.13}$$

7.3. Totally real, metacyclic extensions of $\mathbb{Q}$.

Let $L = \mathbb{Q}$ and let N be a totally real pq-metacyclic extension of $\mathbb{Q}$.

Knowledge of the characters of U_N mean that (equation (6.1)

$$U_N \vee \left(\bigoplus_{i=0}^{q-1} P_i^{(a_i)}\right) \oplus X_T,$$

where $a_i \in \mathbb{N}$, $|T| + a_0 + \cdots + a_{q-1} = q$ and if $T = \emptyset$ then $X_T = \mathbb{S}$.

Write

$$\alpha_i = \begin{cases} 1 & i+1 \notin T, \\ 0 & i+1 \in T, \end{cases}$$

where $0 \in T$ is the same as $q \in T$. Let

$$c_{i+1} = \sum_{k=0}^{i} \alpha_k + a_k,$$

and $c_0 = 0$.

Now, if we know the c_i this would give us more information about the genus of the torsion-free units. The following proposition should give the c_i.

Proposition 7.4. *Let c_i be as above then*

$$\sum_{i=1}^{q-1} \sum_{j=c_i}^{c_{i+1}-1} \sum_{n \equiv j+1}^{i} [\mathbb{F}_p^{(n)}] - [\mathbb{F}_p^{(1)}] = [Cl_N] - [Cl_K], \tag{7.14}$$

in $\mathcal{G}_\Gamma$. The innermost sum is over n such that $j+1 \leq n \leq i$ if $j+1 \leq i$ and over n such that $j+1 \leq n \leq i+q$ otherwise.

Proof. *Using equation (7.4) in* $\mathcal{G}_0^{fd}(\mathbb{Z}\Gamma)$

$$[\Delta S_\infty] = [\mathbb{S}] + 2[P_1] + [P_2] + \dots [P_{q-1}], \tag{7.15}$$
$$= [\mathbb{S}] + [P_1] + \sum_{i=1}^{q-1}[P_i].$$

$$[U_N] = [\mathbb{S}] + \sum_{i=0}^{q-1} a_i[P_i] + \sum_{i\in T}[P_{i-1}], \tag{7.16}$$
$$= [\mathbb{S}] + \sum_{i=0}^{q-1}(a_i + \alpha_i)[P_i].$$

Subtracting (7.15) from (7.16) gives

$$[U_N] - [\Delta S_\infty] = \sum_{i=0}^{q-1}(a_i + \alpha_i - 1)[P_i] + [P_0] - [P_1], \tag{7.17}$$
$$= \sum_{i=0}^{q-1} \sum_{j=c_i}^{c_{i+1}-1} ([P_i] - [P_j]) + [P_0] - [P_1]. \tag{7.18}$$

Map this into $\mathcal{G}_0(\widetilde{K_p\mathcal{C}_q})$ *using* F *and then into* $\mathcal{G}_0^t(\mathbb{Z}_p\mathcal{C}_q)$ *using* ϕ^{-1}.

Now, $[P_i] - [P_{i-1}] \in \mathcal{G}_0^{fd}(\mathbb{Z}\Gamma)$ *maps to* $[\mathbb{F}_p^{(i)}] \in \mathcal{G}_0^t(\mathbb{Z}_p\mathcal{C}_q)$ *and so*

$$[P_i] - [P_{i-a}] \overset{\phi^{-1}\circ F}{\mapsto} \sum_{n=i-a+1}^{i} [\mathbb{F}_p^{(n)}].$$

Hence

$$[P_i] - [P_j] \mapsto \sum_{n\equiv j+1}^{i} [\mathbb{F}_P^{(n)}] \in \mathcal{G}_\Gamma. \quad \square$$

Example: Dihedral extensions of $\mathbb{Q}$.

Let N be a dihedral extension of $\mathbb{Q}$. As there are only two Γ-modules of order p we shall write $\mathbb{F}_p^+$ for $\mathbb{F}_p^{(0)}$ (the module with trivial C_q-action) and $\mathbb{F}_p^-$ for $\mathbb{F}_p^{(1)}$ (non-trivial C_q-action.)

Genus of U_N	c_0	c_1	c_2	$[Cl_N]-[Cl_K]$
$\mathbb{Z}^- \oplus R \oplus R$	0	2	2	$2[\mathbb{F}_p^+]$
$\mathbb{Z}^- \oplus R \oplus P$	0	1	2	$[\mathbb{F}_p^+]$
$\mathbb{Z}^- \oplus P \oplus P$	0	0	2	0
$X \oplus R$	0	1	2	$[\mathbb{F}_p^+]$
$X \oplus P$	0	0	2	0

Notes.

1. *The case where $U_N \vee \mathbb{Z}^- \oplus R \oplus R$ is of particular interest as this is the one case for which an example was not calculated in* [Mol].

   If N/K is ramified then $[Cl_K] \subseteq [Cl_N]$ by proposition 7.3 (i). It is clear that when $U_N \vee \mathbb{Z}^- \oplus R \oplus R$, since $[Cl_N]-[Cl_K] = 2[\mathbb{F}_p^+]$ then

$$h_N/h_K \geq p^2.$$

   Combining this with proposition 1.5 (from [Mol]*) we see that*

$$h_N/h_K = h_k^2/p^2 \geq p^2.$$

   So we must have $h_k \geq p^2$.

   The examples we find in section 9.1 (for dihedral groups of order 6) have

$$h_N = h_k = 9, h_K = 1.$$

2. *As* $[Cl_N] - [Cl_K]$ *is taken modulo* $[\mathbb{F}_p^+] + [\mathbb{F}_p^-]$, *if we write* $h_N/h_k = p^r$ *then*

$$\begin{aligned} r \text{ odd } &\Rightarrow U_N \vee \mathbb{Z}^- \oplus R \oplus P, \\ &\quad \text{or } X \oplus R, \\ r \text{ even } &\Rightarrow U_N \vee \mathbb{Z}^- \oplus R \oplus R, \\ &\quad \text{or } \mathbb{Z}^- \oplus P \oplus P, \\ &\quad \text{or } X \oplus P. \end{aligned}$$

Now using the second equation we found in section 7.2 we get:

Proposition 7.5. *Let* N *be a totally real dihedral extension of* $\mathbb{Q}$. *The genus of* U_N *is exactly determined by*

- $[Cl_N^{\mathcal{C}_p}] - [Cl_K] - m_4[\mathbb{F}_p^+]$
- $[H^1_{\mathcal{C}_p}(\mathcal{P}_S)]$

as follows:

	Genus of U_N	
$[Cl_N^{\mathcal{C}_p}] - [Cl_K] - m_4[\mathbb{F}_p^+]$	$[H^1_{\mathcal{C}_p}(\mathcal{P}_S)] = 0$	$[H^1_{\mathcal{C}_p}(\mathcal{P}_S)] = [\mathbb{F}_p^+]$
$3[\mathbb{F}_p^+]$	—	$\mathbb{Z}^- \oplus R \oplus R$
$2[\mathbb{F}_p^+]$	$\mathbb{Z}^- \oplus R \oplus R$	—
$[\mathbb{F}_p^+]$	$X \oplus R$	$\mathbb{Z}^- \oplus P \oplus R$
0	$\mathbb{Z}^- \oplus P \oplus R$	—
$-[\mathbb{F}_p^+]$	$X \oplus P$	$\mathbb{Z}^- \oplus P \oplus P$
$-2[\mathbb{F}_p^+]$	$\mathbb{Z}^- \oplus P \oplus P$	—

Proof. *Equation (7.13) gives*

$$[H^1_{\mathcal{C}_p}(U_N)] = [H^1_{\mathcal{C}_p}(\mathcal{P}_S)] - [Cl_N^{\mathcal{C}_p}] + [Cl_{N^{\mathcal{C}_p}}] + [H^0_{\mathcal{C}_p}(\mathbb{Z}S_f)].$$

If N *is a dihedral extension then*

$$[H^0_{\mathcal{C}_p}(\mathbb{Z}S_f)] = m_4[\mathbb{F}_p^+]$$

and when N is real then

$$H^1(\mathcal{C}_p, \mathcal{P}_S) \subseteq H^2(\mathcal{C}_p, \mathcal{E}_N) \cong \mathbb{F}_p^+,$$

by equation (4.18), and thus $H^1(\mathcal{C}_p, \mathcal{P}_S) \cong 0$ or $\mathbb{F}_p^+$.

Map equation (7.13) into $\mathcal{G}_\Gamma$ and we get the result. □

Proposition 7.6. *Let N be a complex extension of $\mathbb{Q}$. Then $H^1(\mathcal{C}_p, \mathcal{P}_S) = 0$ by equation (4.18) and so we get*

$[Cl_N^{\mathcal{C}_p}] - [Cl_K] - m_4[\mathbb{F}_p^+]$	*Genus of U_N*
$\mathbb{F}_p^+$	R
$-\mathbb{F}_p^+$	P

□

CHAPTER 8

Addition of torsion units.

Let N be a metacyclic extension of $\mathbb{Q}$ of order pq with units $\mathcal{E}_N$. In this chapter we investigate when the short exact sequence $0 \to \mu_N \to \mathcal{E}_N \to U_N \to 0$ splits. When the order of the Galois group and the torsion units are coprime then the short exact sequence will always split (corollary to theorem 8.1), for example when N is a real, metacyclic extension, but not dihedral.

When N is complex, then using theorem 8.2 it can be shown that the sequence will also always split (lemma 8.3 and theorem 8.5(ii)).

The real dihedral case is the most complicated but in theorem 8.5(i) it is shown that the two possibilities for $\mathcal{E}_N$ depend on the 2-part of the cohomology of $\mathcal{E}_N$ and proposition 8.6 shows that this depends on m_2', the number of primes with ramification group C_2, and how the rational prime p ramifies.

Firstly we prove a proposition that shows $\mathcal{E}_N$ splits in real, non-dihedral extensions.

Theorem 8.1. *Let $0 \to M' \to M \to M'' \to 0$ be an exact sequence of Γ-modules with M'' a lattice. If M' is cohomologically trivial then the sequence splits.*

Proof. *The sequence $0 \to M' \to M \to M'' \to 0$ splits if*

$$\mathrm{Ext_\Gamma}^1(\mathrm{M}'', \mathrm{M}') = \mathrm{H}^1(\Gamma, \mathrm{Hom}(\mathrm{M}'', \mathrm{M}')) = 0.$$

M' is cohomologically trivial implies there exists an exact sequence

$$0 \to B_1 \to B_0 \to M' \to 0$$

with B_0 and B_1 projective lattices. Thus we get an exact sequence

$$\cdots \to H^1(\Gamma, \mathrm{Hom}(M'', B_0)) \to H^1(\Gamma, \mathrm{Hom}(M'', M')) \to H^2(\Gamma, \mathrm{Hom}(M'', B_1)) \to \ldots$$

by lemma 2.4

$$H^i(\Gamma, \mathrm{Hom}(M'', B_j)) = 0.$$

So we get

$$H^1(\Gamma, \mathrm{Hom}(M'', M')) = 0,$$

as required. □

Corollary . *If* $\gcd(|\Gamma|, \mu_N) = 1$ *then the sequence* $\mu_N \to \mathcal{E}_N \to U_N$ *splits.* □

We now give another condition to get a split short exact sequence.

Theorem 8.2. *If* $H^n(\mathcal{C}_q, M'') = 0$ *and* $H^n(\mathcal{C}_p, M') = 0$ *for all* n*, then the sequence* $0 \to M' \to M \to M'' \to 0$ *splits.*

Proof. *As in proposition 8.1, if* M' *is cohomologically trivial as a* $\mathcal{C}_p$*-module so is* $\mathrm{Hom}(M'', M')$ *and,* $H^1(\mathcal{C}_p, \mathrm{Hom}(M'', M')) = 0$.

From lemma 2.4, as M'' *is cohomologically trivial as a* $\mathcal{C}_q$*-module so is* $\mathrm{Hom}(M'', M')$*, and* $H^1(\mathcal{C}_q, \mathrm{Hom}(M'', M')) = 0$.

Since $H^1(\mathcal{C}_p, \mathrm{Hom}(M'', M')) = 0$ *and* $H^1(\mathcal{C}_q, \mathrm{Hom}(M'', M')) = 0$ *we know by theorem 2.2 that*

$$H^1(\Gamma, \mathrm{Hom}(M'', M')) = 0. \quad \square$$

Corollary . *All extensions of* P_i *by* μ_N *split.* □

Combining the previous propositions now shows that $\mathcal{E}_N$ splits whenever N is a non-dihedral, metacyclic extension.

Lemma 8.3. *Let N be a metacyclic extension of $\mathbb{Q}$ of order pq, with p and q odd, then $\mathcal{E}_N \cong U_N \oplus \mu_N$.*

Proof. *If N is real, then $\gcd(|\Gamma|, |\mu_N|) = 1$ and $H^n(\Gamma, \mu_N) = 0$ for all n. So by proposition 8.1, the sequence $0 \to \mu_N \to \mathcal{E}_N \to U_N \to 0$ splits.*

There are no complex extensions with p and q odd. $\square$

We now consider the slightly more complicated dihedral case.

Lemma 8.4. *Let Γ be a dihedral group of order $2p$ and μ_N be the torsion units in a real extension, i.e. ± 1. There are exactly two Γ- extensions of $\mathbb{Z}^-$ by μ_N and of X by μ_N.*

Proof. *We want*

$$\mathrm{Ext_\Gamma}^1(\mathbb{Z}^-, \mu_\mathrm{N}) = \mathrm{H}^1(\Gamma, \mathrm{Hom}(\mathbb{Z}^-, \mu_\mathrm{N})) \cong \mathbb{F}_2,$$

and

$$\mathrm{Ext_\Gamma}^1(\mathrm{X}, \mu_\mathrm{N}) = \mathrm{H}^1(\Gamma, \mathrm{Hom}(\mathrm{X}, \mu_\mathrm{N})) \cong \mathbb{F}_2.$$

Clearly, $\mathrm{Hom}_\Gamma(\mathbb{Z}^-, \mu_N) \cong \mu_N^\Gamma = \mu_N$ and $H^1(\Gamma, \mu_N) \cong \mathbb{F}_2$, so the first part is proved.

Now, X is the non-split extension of $\mathbb{Z}^-$ by R, i.e. we have a short exact sequence

$$0 \to R \to X \to \mathbb{Z}^- \to 0.$$

R is cohomologically trivial under C_2, thus by lemma 2.4 $\mathrm{Hom}(R, \mu)$ is also cohomologically trivial and $H^2(C_2, \mathrm{Hom}(R, \mu) = 0$ for all n

Therefore

$$H^1(C_2, \mathrm{Hom}(X, \mu_N)) \cong H^1(C_2, \mathrm{Hom}(\mathbb{Z}^-, \mu_N)) \cong \mathbb{F}_2.$$

X is cohomologically trivial as a $\mathcal{C}_p$-module, so by lemma 2.4,

$$H^n(\mathcal{C}_p, \mathrm{Hom}(X, \mu_N)) = 0.$$

By theorem 2.2 and since $H^n(\mathcal{C}_p, \mathrm{Hom}(X, \mu_N)) = 0$ we have

$$H^n(\Gamma, \mathrm{Hom}(X, \mu_N)) \cong H^n(\mathcal{C}_2, \mathrm{Hom}(X, \mu_N)).$$

Thus $H^1(\Gamma, \mathrm{Hom}(X, \mu_N)) \cong H^1(\mathcal{C}_2, \mathrm{Hom}(X, \mu_N)) \cong \mathbb{F}_2$ as required. □

Theorem 8.5. *Let N be a dihedral extension of $\mathbb{Q}$.*
(i) If N is real there are exactly two Γ-extensions of U_N by μ_N. Let $\mathcal{E}_N$ be the units of N, then

$$H^{2n}(\Gamma, \mathcal{E}_N)_{(2)} \cong (\mathbb{F}_2)^a$$

where $a = 1$ if the extension splits and 0 if not. (Also, $H^{2n+1}(\Gamma, \mathcal{E}_N)_{(2)} \cong (\mathbb{F}_2)^{a+1}$)

(ii)If N is complex then $\mathcal{E}_N \cong U_N \oplus \mu_N$.

Proof. *(i) Write $U_N \vee U_1 \oplus U_2$ where $U_2 = \mathbb{Z}^-$ or X.*

$$\mathrm{Ext^1}_\Gamma(\mathrm{U_N}, \mu_\mathrm{N}) \cong \mathrm{H}^1(\Gamma, \mathrm{Hom}(\mathrm{U_N}, \mu_\mathrm{N})) \cong$$
$$H^1(\Gamma, \mathrm{Hom}(U_1, \mu_N)) \oplus H^1(\Gamma, \mathrm{Hom}(U_2, \mu_N)) \cong H^1(\Gamma, \mathrm{Hom}(U_2, \mu_N)) \cong \mathbb{F}_2,$$

because U_1 contains only R's and P's which have trivial extensions by μ_N from the corollary to proposition 8.2. Thus there are exactly two extensions of U_N by μ_N.

Let $\mathcal{E}_N = U_1 \oplus \mathcal{E}$ where $0 \to \mu_N \to \mathcal{E} \to U_2 \to 0$ is an exact sequence.

If the extension splits then $H^{2n}(\Gamma, \mathcal{E}_N)_{(2)} = H^{2n}(\Gamma, \mu_N)_{(2)} \oplus H^{2n}(\Gamma, U_1)_{(2)} \oplus H^{2n}(\Gamma, U_2)_{(2)}$. Calculating this gives $a = 1$.

We shall find the structure of the non-split extension. Write $\mathcal{E} = \{(m, u) | m \in \mu_N, u \in U_2\}$ and $\tau(m, u) = (m', u')$. Now $\mathcal{E}/\mu_N \cong U_2$, so $\tau(m, u) = (m', \tau(u))$.

If $m' = m$ then we will get the split extension. The only other possibility is that $m' = -m$, and $\tau(m,u) = (-m, \tau(u))$.

It is clear that $\mathcal{E}^\Gamma = 0$ implying $H^0(\Gamma, \mathcal{E}) = 0$. So $H^{2n}(\Gamma, \mathcal{E}_N) = H^{2n}(\Gamma, U_1) \oplus H^{2n}(\Gamma, \mathcal{E}) = 0$ and $a = 0$.

(ii) Since U_N is either R or P this is just the corollary to proposition 8.2. □

Proposition 8.6. *Let N be a real dihedral extension of $\mathbb{Q}$ of order $2p$. If $2 \nmid h_N$ then $\mathcal{E}_N \cong U_N \oplus \mu_N$ if and only if (i) p ramifies totally (i.e. $(p) = \mathcal{P}^{2p}$ in N) and at least one prime ramifies with decomposition group C_2 or (ii) two primes ramify with decomposition group C_2.*

Proof. $|H^2(\Gamma, U_N)|_{(2)} = 1$ *so by equation (4.18),* $|H^1(\Gamma, \mathcal{P}_S)|_{(2)} = 1$.

From the 2-part of equation (5.8) (with $\Omega = \Gamma$ and rearranging) we can actually get a stronger result than the one stated in the lemma

$$|H^1(\Gamma, \mathcal{E}_N)|_{(2)} = \frac{[\mathbb{Z}S_f{}^\Gamma : \mathbb{Z}\hat{S}]_{(2)}}{|Cl_N|_{(2)}}. \tag{8.1}$$

Looking at the case when $2 \nmid h_N$ then

$$|H^1(\Gamma, \mathcal{E}_N)|_{(2)} = [\mathbb{Z}S_f{}^\Gamma : \mathbb{Z}\hat{S}]_{(2)} = 2^{a+1},$$

which is $2^{m_2'}$ if p does not ramify totally, and $2^{m_2'+1}$ if it does. □

CHAPTER 9

Examples and discussion.

9.1. Examples of dihedral extensions of order 6.

The following examples are for dihedral extensions N of $\mathbb{Q}$ of degree 6 (with Galois group $\Gamma = C_3 \rtimes C_2$) generated by the roots of the cubic equations listed.

$K = N^{C_3}$ is a quadratic extension of $\mathbb{Q}$ and $k = N^{C_2}$ is a non-Galois, cubic extension. m_4, m_3 and m_2 are the number of ramified primes with decomposition groups Γ, C_3 and C_2 respectively.

The structure of the class groups is written as $[n_1, \ldots, n_l]$ which means it is a product of cyclic groups of order n_i.

Example	Cl_N	Cl_K	Cl_k	m_4	m_3	m_2	*Equation*	*Genus of* U_N
1	[1]	[3]	[1]	0	0	1	$x^3 - 4x + 1$	$X \oplus R$
2	[1]	[3]	[1]	0	0	2	$x^3 - 3x^2 - 17x - 2$	$X \oplus R$
3	[1]	[1]	[1]	1	0	1	$x^3 + 3x^2 - 9x + 2$	$X \oplus P$
4	[1]	[1]	[1]	1	0	1	$x^3 + 3x^2 - 18x - 2$	$X \oplus P$
5	[2]	[2]	[1]	1	0	2	$x^3 - 18x - 20$	$X \oplus P$
6	[1]	[1]	[1]	2	0	1	$x^3 - 9x^2 + 15x - 3$	$\mathbb{Z}^- \oplus P \oplus P$
7	[9]	[27]	[1]	0	0	1	$x^3 - 13x + 1$	$X \oplus R$
8	[3,3]	[1]	[3]	3	0	1	$x^3 - 60x - 20$	$\mathbb{Z}^- \oplus P \oplus P$
9	[6]	[2]	[3]	0	1	2	$x^3 - 12x + 1$	$X \oplus R$
10	[3]	[1]	[3]	1	1	1	$x^3 + 15x^2 + 12x - 15$	$\mathbb{Z}^- \oplus R \oplus P$
11	[3]	[1]	[3]	1	1	1	$x^3 - 27x^2 - 9x + 6$	$\mathbb{Z}^- \oplus R \oplus P$
12	[3,3]	[1]	[3,3]	0	2	1	$x^3 + 15x^2 - 9x - 8$	$\mathbb{Z}^- \oplus R \oplus R$
13	[3,3]	[1]	[3,3]	0	2	2	$x^3 + 36x^2 - 30x - 29$	$\mathbb{Z}^- \oplus R \oplus R$

Note. *Using lemma 8.6 we see that in example 13 $\mathcal{E}_N$ splits into $U_N \oplus \mu$ and in example 12 it does not.*

9.2. Examples of Siegel units.

Let M be a positive integer and $\Gamma(M) = \left\{\alpha = \left(\begin{smallmatrix} a & b \\ c & d\end{smallmatrix}\right) \middle| \, \alpha \equiv \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1\end{smallmatrix}\right) mod M\right\}$.

Definition. *A* **modular function of level** *M is a function $h\binom{\omega_1}{\omega_2}$ of two complex variables such that*

MF1. $h\left(\lambda\binom{\omega_1}{\omega_2}\right) = \lambda^k h\binom{\omega_1}{\omega_2}, \quad \lambda \in C^*$

for some fixed $k \in \mathbb{Z}$ (called its weight.)

MF2. $h\left(\alpha\binom{\omega_1}{\omega_2}\right) = h\binom{\omega_1}{\omega_2}$ *for all $\alpha \in \Gamma(M)$.*

MF3. *For $\tau \in \mathfrak{H}$, the upper-half plane, the function $h\binom{\tau}{1}$ is meromorphic at infinity.*

Let F_M be the modular function field of modular functions of level M over $\mathbb{Q}$. $j = j(L)$ is the **classical modular function**

$$j = 2^6 \cdot 3^3 g_2^3 / g_2^3 - 2g_3^2, \tag{9.1}$$

where $g_2 = 60 \sum_{\omega \in L'} \omega^{-4}, g_3 = 140 \sum_{\omega \in L'} \omega^{-6}$ for a lattice L, L' is L without zero.

Theorem 9.1. *([La], p.66, theorem 3) The Galois group of $F_M/\mathbb{Q}(j)$ is*

$$GL_2(\mathbb{Z}/M\mathbb{Z})/\pm 1. \quad \square$$

We are interested in the case when M is 2 because then the Galois group is dihedral of order 6.

Let $a = (r/M, s/M)$ where r and s are integers not both divisible by M. If this is the smallest such M then we say a has **precise denominator** *M.*

Definition. *Let $\tau \in \mathfrak{H}$. Define the* **Siegel functions** *by*

$$g_a(\tau) = \mathfrak{k}_a(\tau)\Delta(\tau)^{1/12}, \tag{9.2}$$

where

- $\Delta(\tau)^{1/12}$ *is the square of the Dedekind eta function*

$$\eta(\tau)^2 = 2\pi i \xi_\tau^{1/12} \prod_{n=1}^{\infty} (1 - \xi_\tau^n)^2,$$

  where $\xi_\tau = e^{2\pi i \tau}$.

- $\mathfrak{k}(\tau)$ *are Klein forms,*

$$\mathfrak{k}(\tau) = e^{-\eta(z,L)z/2} \sigma(z, L).$$

  where L *is the lattice* $[\tau, 1]$ *and* $z = r/M\tau + s/M$.

- $\sigma(z, L)$ *is the Weierstrass sigma function*

$$\sigma(z, L) = z \Pi_{\omega \in L'} (1 - z/\omega) e^{z/\omega + 1/2(z/\omega)^2},$$

  where L' *is* L *without zero.*

Then g_a *is a modular function and the* ξ_τ*-expansion of* g_a^{12M} *is given by*

$$\xi_\tau^{N+6s+6s^2/M} \xi_M^{-6rs} (\xi_M^r \xi_\tau^{-s/M} - 1)^{12M} \prod_{n=1}^{\infty} [(1 - \xi_\tau^{n-s/M} \xi_M^r)(1 - \xi_\tau^{n+s/M} \xi_M^{-r})]^{12M} \quad (9.3)$$

where $\xi_\tau = e^{2\pi i \tau}$ *and* $\xi_M = e^{2\pi i/M}$.

Theorem 9.2. *(*[KL]*, p.37, theorem 2.2) Let a have precise denominator* M*, then*
(i) If M *is composite, then* g_a^{12M} *is a unit over* $\mathbb{Z}$.
(ii) If $M = p^r$ *is a prime power, then* g_a^{12M} *is a unit in* $R_M[1/p]$*, (*R_M *is the integral closure of* $\mathbb{Z}[j]$ *in* F_M*.)*
(iii) If $c \in \mathbb{Z}, c \neq 0$ *is prime to* M*, then* $(g_{ca}/g_a)^{12M}$ *is a unit over* $\mathbb{Z}$. □

Theorem 9.3. *(*[KL]*, p.41, theorem 3.1) The rank of the group generated by the Siegel functions modulo constants* g_a *for* $a \in 1/M\mathbb{Z}^2/\mathbb{Z}^2$ *mod* ± 1 *is equal to* $|c(M)/\pm 1| - 1$ *where* $GL_2(M) = c(M)G_\infty(M)$*, and* $G_\infty(M)$ *is the isotropy group of* $\binom{1}{0}$. □

Combining theorems 9.2 and 9.3 we see in the case when M *is 2 and* $j \in \mathbb{Z}$ *the Siegel functions generate a subgroup of the units of* $\mathbb{Z}$*-rank 2.*

Theorem 9.4. *([La], p263, theorem 2) The Siegel functions g_a^{12M} ($a \in \mathbb{Q}^2, a \notin \mathbb{Z}^2, a$ has precise denominator M) lie in F_M and generate F_M over $\mathbb{Q}(j)$. They are integral over $\mathbb{Z}[j]$ and are roots of the following polynomial in $\mathbb{Z}[j][x]$*

$$\prod(x - g_a^{12M}), \tag{9.4}$$

where the product is over all a $\bmod (\mathbb{Z}^2)$ with precise denominator M. □

We now calculate polynomial (9.4) for $M = 2$. It is clearly cubic (there are three distinct a with precise denominator $2 \mod (\mathbb{Z}^2)$) and the ξ_τ-expansion of j is

$$j = 1/\xi_\tau + 744 + 196,884\xi_\tau + 21,493,760\xi_\tau^2 + \ldots \tag{9.5}$$

Equating the coefficients of ξ_τ we get the polynomial

$$x^3 + (2j + 2^8 \cdot 3)x^2 + (j^2 - 2^9 \cdot 3j + 2^{16} \cdot 3)x + 2^{24}. \tag{9.6}$$

Substitute $j' = 2^{-18}j$ and $X = 2^{-8}x$ in polynomial (9.6) to get

$$\boxed{X^3 + (2j' + 3)X^2 + (j'^2 - 6j' + 3)X + 1}. \tag{9.7}$$

Then $\mathbb{Q}(j) = \mathbb{Q}(j')$ and the extension F_2 formed by adding the roots of (9.6) is the same as that for (9.7). When $j \in \mathbb{Z}$ the roots of (9.7)(which are $g_a^{24}/2^8$) are units over $\mathbb{Z}$ in F_2, call these s_1, s_2, s_3.

We shall calculate some examples of these and find the torsion part of $U_N/\langle s_1, s_2, s_3\rangle$. It is clear from the action of the Galois group on the roots and the fact that $s_3 = 1/s_1 s_2$ that $\langle s_1, s_2, s_3\rangle \vee R$.

Real examples

Example	j'	m_4	m_3	m_2	Cl_N	*Torsion*	*Genus of* U_N
14	10	2	0	1	[1]	12	$\mathbb{Z}^- \oplus P \oplus P$
15	11	1	0	1	[1]	12	$X \oplus P$
16	12	2	0	1	[1]	12	$\mathbb{Z}^- \oplus P \oplus P$
17	17	1	0	1	[1]	12	$X \oplus P$
18	29	1	0	1	[4]	12	$X \oplus P$
19	31	0	1	1	[3]	12	$\mathbb{Z}^- \oplus R \oplus P$

Complex examples

Example	j'	m_4	m_3	m_2	Cl_N	*Torsion*	*Genus of* U_N
20	-3	1	0	1	[4]	12	P
21	1	0	0	1	[1]	36	R
22	4	1	0	1	[1]	48	P

In all the real examples $\langle s_1, s_2, s_3 \rangle$ *is contained inside* P. *Since it is in the same genus as* R *we know that 3 must divide the torsion. 4 also divides the torsion in all these examples, and the following proposition proves this is always true.*

Proposition 9.5. *If* s_1, s_2, s_3 *are the roots of the equation*

$$x^3 + (2j' + 3)x^2 + (j'^2 - 6j' + 3)x + 1 = 0,$$

and $Gal(\mathbb{Q}(s_1, s_2, s_3)/\mathbb{Q}) \cong D_3$ *then* $i\sqrt{s_1}, i\sqrt{s_2}, i\sqrt{s_3}$ *are all contained in* $\mathbb{Q}(s_1, s_2, s_3)$.

Proof. $\pm i\sqrt{s_1}, \pm i\sqrt{s_2}, \pm i\sqrt{s_3}$ *are roots of the equation*

$$y^6 - (2j' + 3)y^4 + (j'^2 - 6j' + 3)y^2 - 1,$$

and this factorizes as

$$(y^3 - 3y^2 + (3 - j')y - 1)(y^3 + 3y^2 - (3 - j')y + 1). \tag{9.8}$$

Then $\mathbb{Q}(s_1, s_2, s_3)$ *is contained in the extension generated by the roots of one of these cubics. The Galois group is* D_3 *so the two extensions are the same.* □

9.3. Discussion.

In all the examples calculated, examples with the same values of m_2, m_3 *and* m_4 *have the same genus (but these calculations only include class groups of order 9 or less). It is doubtful this is true in general, but perhaps a combination of the class group and* m_2, m_3, m_4 *could uniquely determine the genus? It is also interesting to note that all the possible genera which could occur given that* $U_N \otimes \mathbb{Q} \cong \Delta S_\infty \otimes \mathbb{Q}$ *do occur. In general, does the number of genera of units reach the limit given in proposition 6.2?*

It would be of interest to know for which other groups the characters and cohomology determine the genus of a lattice.

Bibliography

[Br] K. Brown, "Cohomology of Groups", Graduate Texts in Math. 87, Springer-Verlag, New York, 1982.

[Bu] D. Burns, *On the Galois structure of units in number fields*, Proc. London Math. Soc., **66** (1993), 71-91.

[CR1] C. Curtis, I. Reiner, "Methods of Representation Theory", Volume 1, J.Wiley and Sons, New York, 1981.

[Du] D. Duval, *Galois structure of units of a real type* (p,p) *abelian field*, J. of No. Theory, **13** (1981), 228-245.

[Fr] A. Fröhlich, *Units in real, abelian fields*, J. reine angew. Math., **429** (1992), 191-217.

[Ge] F. Gerth III, *Cubic fields whose class numbers are not divisible by* 3, Illinois J. Math. **20** (1976), 486-493.

[GW1] K.W. Gruenberg, A. Weiss, *Galois invariants for units*, Proc. London Math. Soc., **70,2** (1995) 264-284.

[GW2] —, *Galois invariants for local units*, Quarterly J. of Math., **47** (1996), 25-39.

[Ho] D. Holland, *Chinburg's third invariant in the factorizability defect class group*, Canadian J. of Math., **46,2** (1994), 324-342.

[HW1] D. Holland, S.M.J. Wilson, *Localization and class groups of module categories with exactness defect*, Math. Proc. of the Cambridge Philosophical Soc., **113** (1993), 233-251.

[HW2] —, *Factor equivalence of rings of integers and Chinburg's second invariant in the defect class group*, J. of the London Math. Soc., **49** (1994), 417-441.

[Ja1] J-F. Jaulent, *Sur la l-structure galoisienne des idéaux ambiges dans une extension métacyclique de degré nl sur le corps des rationnels*, Pub. Math. Fac. Sc. Besançon, (1979-1980).

[Ja2] —, *Unités et classes dans les extensions métabéliennes de degré* nl^s *sur un corps de nombres algébriques*, Ann. Inst. Fourier, Grenoble, **31,1** (1981), 39-62.

[Ja3] —, *Sur la* $\mathbb{Z}_l[G]$*-structure des unités principales d'un corps local et des unités globales d'un corps de nombres à groupe de Galois métacyclique*, Abh. Math. Sem. Hamburg, **52** (1982), 235-253.

[KL] D. Kubert, S. Lang, "Modular Units", Grundlehren der mathematischen Wissenschaften 244, Springer-Verlag, New York, 1981.

[La] S. Lang, "Elliptic Functions", Addison Wesley, 1974.

[Le] M.P. Lee, *Integral Representations of Dihedral Groups of Order* $2p$, Trans. Amer. Math. Soc., **110** (1964), 213-231.

[Ma1] R. Marszalek, *Minkowski units in certain metacyclic fields*, Acta Arithmetica, (1988), 381-391.

[Ma2] —, *Minkowski units in a class of metabelian fields*, J. of No. Theory, **37** (1991), 67-91.

[Mc] S. MacLane, "Homology", Springer-Verlag, Berlin, 1963.

[Mo1] N. Moser, *Unités et nombres de classes d'une extension Galoisienne diédrale de* $\mathbb{Q}$, Abh. Math. Sem. Univ. Hamburg, **48** (1979), 54-75.

[Mo2] —, *Sur les unités d'une extension galoisienne non abelienne de degré pq du corps des rationnels, p et q nombres premiers impairs*, Ann. Inst. Fourier, Grenoble, **29,1** (1979), 137-158.

[Pu] L.C. Pu, *Integral representations of non-abelian groups of order pq*, Michigan Math. J., **12** (1965), 231-246.

[Ri] P. Ribenboim, "Algebraic Numbers", J.Wiley and Sons, New York, 1972.

[Se] J-P. Serre, "Local Fields", Graduate Texts in Math. 67, Springer-Verlag, New York, 1979.

[Sy] P. Symonds, *Cohomological methods in integral representation theory*, J. of Pure and Applied Algebra, **56** (1989), 163-176.

[Ta] J. Tate, *Les Conjectures de Stark sur les Fonctions L d'Artin en* $s = 0$, Progress in Math, **47**, Birkhäuser (1984).