The Structure of the Hilbert Symbol for Unramified Extensions of 2-adic Number Fields

Lloyd D.Simons

Department of Mathematics

McGill University, Montreal

March, 1986

A thesis submitted to the Faculty of Graduate Studies and Research
in partial fulfillment of the requirements for the degree of Doctor of Philosophy.

The Structure of the Hilbert Symbol for Unramified Extensions of 2-adic Number Fields.

Abstract

Let G be a finite Abelian group with cyclic 2-Sylow subgroup. In the first part of this thesis, we obtain a structure theorem for nondegenerate, anti-symmetric, G-invariant bilinear forms on a free $\mathbb{F}_2[G]$-module of finite type. This theorem is then applied to determine the structure of the Hilbert symbol on an unramified extension K of a 2-adic number field k, in the case where K doesn't contain the fourth roots of unity.

If k is an irregular p-adic number field, and $k(p)$ is the maximal p-extension of k, then the Galois group $X = \mathrm{Gal}(k(p)/k)$ is a Demuškin group, and the maximal unramified Abelian extension T of k determines a "$\mathbb{Z}_p$-tower" in X. The second part of this thesis endeavors to classify $\mathbb{Z}_p$-towers in Demuškin groups. For $p \neq 2$ and in certain cases when $p = 2$, a complete classification is found, and in the remaining cases some necessary invariants are given.

La Structure du Symbole de Hilbert pour les Extensions Non Ramifiées d'un Corps 2-adique.

Résumé

Soit G un groupe Abélien fini dont le 2-groupe de Sylow est cyclique. Dans la première partie de cette thèse, on obtient une classification de formes bilinéaires, non dégénérées, non symétriques, et invariantes par G, sur une éspace $\mathbb{F}_2[G]$-libre de type fini. Ensuite, on applique cette théorie pour détérminer la structure du symbole de Hilbert pour ces extensions K non ramifiées d'un corps 2-adique k, dont K ne contient pas les racines quatrièmes de l'unité.

Soit k un corps p-adique irrégulier, et soit $k(p)$ la plus grande extension de k dont le groupe de Galois X est un pro-p groupe. X est donc un groupe de Demuškin , et si T est la plus grande extension non ramifiée de k contenue dans $k(p)$, T donne "un tour de $\mathbb{Z}_p$ dans X". Dans la dieuxième partie de cette thèse, on se propose de classer les tours $\mathbb{Z}_p$ dans les groupes de Demuškin . Pour les cas où $p \neq 2$, ét quelquefois pour $p = 2$, on donne une classification complète. En ce qui concerne les autres cas, on propose quelques invariants qui pourraient éventuellement intervenir dans la classification.

Table of Contents

Introduction

Let k be a p-adic number field, and let T be the maximal tamely ramified extension of k—T/k is Galois, and the structure of the Galois group $\mathcal{G}$ was determined by Hasse and Iwasawa. Let K/k be an intermediate field which is finite and normal over k with Galois group G, and assume that K is irregular—K contains the p^{th} roots of unity.

In [Ko 1], H. Koch examined the Hilbert symbol on the $\mathbb{F}_p$-vector space $K^{\times}/K^{\times p}$ as a G-invariant symplectic form, and for $p \neq 2$ was able to determine the structure of this form in a particularly nice way. This structure theorem was extended by Jakovlev in [Ja 1]–[Ja 4], and became the principal ingrediant in Jakovlev's construction of the absolute Galois group of k in [Ja 3]. Following Koch and Jakovlev, Želvinskii was able to obtain a similar structure theorem for the Hilbert symbol on tamely ramified extensions K of 2-adic number fields when K contains the fourth roots of unity, and in [Z 1] used this theorem to construct the absolute Galois group of those 2-adic number fields k whose maximal tamely ramified extension T contains the fourth roots of unity.

In [Ko 4], Koch gave a very elegant axiomatic description of the absolute Galois group X_k of the p-adic number field k (in the case $p \neq 2$) by introducing the notion of a "Demuškin formation over $\mathcal{G}$"; Inspired by Koch's work, U. Jannsen and K. Wingberg were able to give a finite presentation of X_k ([JW 1]). Following Jannsen and Wingberg, and using the results of [Z 1], V. Diekert was able to give a similar presentation of X_k for those 2-adic number fields k whose maximal tamely ramified extension contain the fourth roots of unity.

When k is a 2-adic number field whose maximal tame extension does not contain the fourth roots of unity, the only published result known to this author is due again to Koch: in [Ko 3], a classification theorem is given for the symplectic structure of the Hilbert symbol for unramified extensions of k of 2-power order.

In chapter 1 of this thesis, we classify anti-symmetric, G-invariant, bilinear forms on finitely generated free $\mathbb{F}_2[G]$-modules, where G is an Abelian group with cyclic 2-Sylow subgroup, the main result being Proposition 1.11: such non-alternating forms satisfying a "trace condition" are determined up to isometry by the rank of the space, and by what we call their "Koch invariant" ι, which is either 0 or 1. In chapter 2 we apply our structure theorem to the main object of interest: the Hilbert symbol on unramified extensions K of 2-adic number fields k, in the case where K does not contain the fourth roots of unity. Our main contribution appears as the Corollary to proposition 2.3.

Chapter 3 contains some more or less known material on Demuškin groups and their cohomology. In chapter 4, we define the notion of a "$\mathbb{Z}_p$-tower" in a Demuškin group, and for $p \neq 2$ (and, of course, some cases when $p = 2$), we obtain a complete classification of these towers (proposition 4.2), using in an essential way the Koch/Wingberg/Diekert uniqueness theorem for Demuškin formations.

The motivational germ for the work in this thesis was the desire to formulate an adequate definition of a Demuškin formation over $\mathcal{G}$ which could be identified with the absolute Galois group of those 2-adic number fields whose maximal tame extension doesn't contain the fourth roots of unity. In the last two sections of chapter 4, we define some invariants of $\mathbb{Z}_2$-towers in Demuškin groups which must be considered in any such definition, and give some examples.

The author wishes to thank J. P. Labute and H. Kisilevsky for bringing to my attention the work of Jannsen and Wingberg on Demuškin formations; and U. Jannsen, R. Foote, and D. Dummit for some enlightening discussions. The author also wishes to thank the J.W.McConnell Foundation for their generous support.

Notation

$\mathbf{Q}$	the rational numbers
$\mathbf{Z}$	the rational integers
$\mathbf{Q}_p$	the field of rational p-adic numbers
$\mathbf{Z}_p$	the ring of rational p-adic integers
$R^{\times}$	the multiplicative group of the ring R
R^{+}	the additive group of the ring R
$R[G]$	the group algebra of the group G with coefficients in the ring R
A^{G}	the submodule of the G-module A whose elements are fixed by G
$\operatorname{tor}(A)$	the torsion submodule of A
${}_qA$	the submodule of A of elements of exponent q
A^{*}	the Pontrjagin dual of A: $\operatorname{Hom}(A, \mathbf{Q}/\mathbf{Z})$
$X^{(i,q)}$	the i'th term in the lower q-central series of the group X

Chapter 1. G-Invariant Bilinear Forms

§ 1.1 Let k be a commutative ring, and let R be a k-algebra with involution '$*$' satisfying for all $\lambda,\mu \in R$: $(\lambda\mu)^* = \mu^*\lambda^*$, $(\lambda^* + \mu^*) = (\lambda + \mu)^*$, and $(\lambda^*)^* = \lambda$. An R-invariant form Φ on the R-module M is a k-bilinear form $: M \times M \to k$ such that for all $v_1, v_2 \in M$ and $\lambda \in R$,

$$\Phi(\lambda v_1, v_2) = \Phi(v_1, \lambda^* v_2).$$

We will use the notation (M, Φ) to denote the space M with the form Φ if ambiguity would result by using M alone.

As usual, the bilinear form Φ is said to be symmetric (respectively, antisymmetric) if for all $v_1, v_2 \in V$, one has $\Phi(v_1, v_2) = \Phi(v_2, v_1)$ (resp.,$\Phi(v_1, v_2) = -\Phi(v_2, v_1)$); a vector $v \in V$ is said to be isotropic if $\Phi(v, v) = 0$, and the form Φ is called alternating if every vector is isotropic. Note that an alternating form is always antisymmetric: $0 = \Phi(v_1 + v_2, v_1 + v_2) = \Phi(v_1, v_2) + \Phi(v_2, v_1)$; if 2 is invertible in k, then the converse is true. A form is non-alternating if it possesses a non-isotropic vector. In the sequel, we will concern ourselves only with symmetric and antisymmetric forms.

Given a vector $w \in V$, let $w^\perp = \{v \in V : \Phi(w, v) = 0\}$, and for $W \subset V$, let $W^\perp = \cap_{w \in W} w^\perp$. Note that if W is an R-submodule of V, then so is $W^\perp$. The subset W is called totally isotropic if $W^\perp \supset W$. The form Φ is nondegenerate on V (more precisely, nondegenerate on the left, but for our purposes left- and right- nondegeneracy are equivalent) if $V^\perp = \{0\}$. In this case, we will say that V is complete. Let V and W be complete spaces with R-invariant forms Φ and Ψ. An isometry of these spaces is an R-isomorphism $f: V \to W$ such that for all $v_1, v_2 \in V$,

$$\Psi(f(v_1), f(v_2)) = \Phi(v_1, v_2).$$

Two such forms are called isometric or equivalent.

Any k-bilinear form Φ on the R-module V defines a homomorphism

$$f_\Phi : V \to \mathrm{Hom}_k(V, k), \quad f_\Phi(v)(w) = \Phi(v, w). \tag{1.1}$$

If we let R act on $\mathrm{Hom}_k(V, k)$ by the rule $(\lambda f)(v) = f(\lambda^* v)$, then the R-invariance of Φ implies that f_Φ is a homomorphism of R-modules; if f_Φ is an isomorphism, the form Φ is said to be non-singular (on the left). When k is a field or a local ring, and V is finitely generated over k, then (left-) non-singular and (left-) nondegenerate are equivalent.

The complete space V is said to decompose as the sum of complete spaces V_1 and V_2 if there exists a module decomposition $V \cong V_1 \oplus V_2$ such that the form Φ restricts to a nondegenerate form on the V_i, and $\Phi(v_1, v_2) = 0$ for all $v_i \in V_i$. We will call the complete space V simple if no such decomposition exists. Conversely, if Φ_i is an R-invariant form on the complete space M_i for $1 \leq i \leq t$, define the 'sum' of the spaces M_i to be the space $M = \oplus M_i$ with form Φ defined by

$$\Phi(\sum_i v_i, \sum_j v_j') = \sum_i \Phi_i(v_i, v_i'),$$

for v_i, $v_i' \in M_i$.

Lemma 1.1. *Let k be a field or a local ring, and let V be a finitely generated R-module which is of finite rank over k. Let Φ be a nondegenerate, antisymmetric form on V, and suppose that $W \subset V$ is a R-submodule such that the restriction of Φ to W is nondegenerate. Then V decomposes as a sum of complete subspaces $W \oplus W^{\perp}$.*

PROOF Let $v \in V$, and let $f_v \in \mathrm{Hom}_k(W, k)$ be the restriction of $f_\Phi(v) \in \mathrm{Hom}_k(V, k)$ to W. Since Φ is nondegenerate on W, there is a $w \in W$ such that $f_\Phi(w) = f_\Phi(v)$ on W. Let $w' = v - w$, so that $f_\Phi(w') = f_\Phi(v) - f_\Phi(w)$ vanishes on W,and hence $w' \in W^{\perp}$. It follows that $V = W + W^{\perp}$, and this sum is direct, since

$$\{0\} = V^{\perp} = (W + W^{\perp})^{\perp} = W^{\perp} \cap W.$$

Since Φ is nondegenerate on V and on W, it must restrict to a nondegenerate form on $W^{\perp}$ as well.◇

Let M be an R-module with nondegenerate, anti-symmetric form Φ. We will say that M possesses a "hyperbolic decomposition" if there exist submodules M_1, M_2 of M such that $M = M_1 \oplus M_2$ as R-modules, and the restriction of Φ to each of the spaces M_i is totally isotropic.

Lemma 1.2. *Suppose that k is a field, and that M is an R-module which is finite dimensional over k. Let $M = M_1 \oplus M_2$ give a hyperbolic decomposition of M for each of the two nondegenerate, R-invariant, anti-symmetric forms Φ and Ψ. Then there exists an isometry between (M, Φ) and (M, Ψ).*

PROOF Let f_Φ denote the composition,

$$M_2 \longrightarrow M \xrightarrow{f_\Phi} \mathrm{Hom}(M,k) \xrightarrow{res} \mathrm{Hom}(M_1,k).$$

f_Φ is certainly an A-homomorphism. It is injective, for if $v_2 \in M_2$ and $f_\Phi(v_2) = 0$, then $f_\Phi(v_2) = 0$ (since M_2 is totally isotropic) and hence $v_2 = 0$. Thus $\dim_k M_2 \leq \dim_k \mathrm{Hom}(M_1,k) = \dim_k M_1$. Defining in a similar manner $g_\Phi : M_1 \to \mathrm{Hom}(M_2,k)$ shows that $\dim_k M_1 \leq \dim_k \mathrm{Hom}(M_2,k)$. It follows that f_Φ is an isomorphism. Define f_Ψ in the same way, and let

$$\theta_2 : M_2 \to M_2, \quad \theta_2(v) = f_\Psi^{-1} \circ f_\Phi(v).$$

Extend θ_2 to an isomorphism θ of M onto itself by the identity on the submodule M_1. For $v = v_1 + v_2$ and $w = w_1 + w_2$ in M, we have,

$$\begin{aligned}\Psi(\theta(v),\theta(w)) &= \Psi(v_1 + \theta(v_2), w_1 + \theta(w_2))\\ &= \Psi(v_1, \theta(w_2)) + \Psi(\theta(v_2), w_1)\\ &= -f_\Psi(\theta(w_2))(v_1) + f_\Psi(\theta(v_2))(w_1)\\ &= -f_\Phi(w_2)(v_1) + f_\Phi(v_2)(w_1)\\ &= \Phi(v,w).\end{aligned}$$

Thus θ gives an isometry.◇

§ 1.2 In this section, we will suppose that G is a cyclic group of prime power order $q = p^e$ generated by the element σ. Let A be the group ring $\mathbb{F}_p[G|$, and define the involution '$*$' by the rule

$$(\sum_{g \in G} a_g g)^* = \sum_{g \in G} a_g g^{-1}.$$

One easily checks that the $\mathbb{F}_p$-algebra A is a ring with involution in the sense of §1.1. If Φ is an $\mathbb{F}_p$-bilinear form on the A-module M, then Φ is said to be "G-invariant" if for all $g \in G$ and $x,y \in M$ one has

$$\Phi(g.x, g.y) = \Phi(x,y).$$

A simple calculation shows that a G-invariant form is A-invariant (for the involution $*$).

Lemma 1.3. *Λ is a local ring whose maximal ideal $\mathcal{M}$ is principal, generated by the element $\pi = \sigma - 1$. The powers of $\mathcal{M}$ are stable under the involution $*$, and the powers of π form an $\mathbf{F}_p$-basis for Λ; the "norm-element" of the group ring Λ is*

$$Sp_G = \sum_{g \in G} g = \pi^{q-1}.$$

PROOF The augmentation map $\varepsilon : \Lambda \rightarrow \mathbf{F}_p$, defined by mapping $\sigma \mapsto 1$ and extending to a ring homomorphism, has kernel $\mathcal{M}$ generated by $\sigma^{q} - 1 = (\sigma - 1)(1 + \sigma + \ldots + \sigma^{q-1})$, hence $\mathcal{M}$ is principal. Notice that Λ is the homomorphic image of $\mathbf{F}_p[X]$ under the map $X \mapsto \sigma - 1 = \pi$, with the kernel generated by $(1+X)^q - 1 = X^q$; since $1, X, \ldots, X^{q-1}$ clearly gives a basis of $\mathbf{F}_p[X]/X^q$, it follows that the powers of π give a basis of the $\mathbf{F}_p$-vector space Λ. In $\mathbf{F}_p[X]$, one has

$$1 + (1+X) + (1+X)^2 + \ldots + (1+X)^{q-1} = \frac{(1+X)^q - 1}{(1+X) - 1} = \frac{(1+X^q) - 1}{X} = X^{q-1},$$

so that in Λ, $\pi^{q-1} = Sp_G$. Sp_G is certainly fixed under $*$, so if $u \in \Lambda^{\times}$, then $(Sp_G u)^* = u^* Sp_G$ and hence $u^* \in \Lambda^{\times}$. It now follows that if $\pi^* = \pi^t v$ with v a unit, then $Sp_G^* = (\pi^{q-1})^* = (\pi^*)^{q-1} = (\pi^t)^{q-1} v^{q-1}$, so that $t = 1$, and the powers of $\mathcal{M}$ are stablised.◇

For any $x \in \Lambda$, we can write $x = \pi^{\mathrm{ord}_\pi(x)} u$ with $u \in \Lambda^{\times}$, uniquely defining the "grading function" ord_π. For the remainder of this section, we will assume that p is an odd prime.

Lemma 1.4. *Let Φ be a nondegenerate, anti-symmetric form on the Λ-module M. If $\chi \in M$, then $\Phi(\chi, Sp_G \chi) = 0$.*

PROOF We can write

$$Sp_G = \pi^{q-1} = \pi^{\frac{q-1}{2}} \pi^{\frac{q-1}{2}} = \pi^{* \frac{q-1}{2}} \pi^{\frac{q-1}{2}} u,$$

with $u \in \mathbf{F}_p$. Thus,

$$\begin{aligned} \Phi(\chi, Sp_G \chi) &= \Phi(\chi, \pi^{* \frac{q-1}{2}} \pi^{\frac{q-1}{2}} u \chi), \\ &= \Phi(\pi^{\frac{q-1}{2}} \chi, u \pi^{\frac{q-1}{2}} \chi), \qquad (1.2) \\ &= 0. \diamond \end{aligned}$$

Proposition 1.1. *Let M be a free Λ-module of rank n, with Φ a nondegenerate, anti-symmetric form on M. Then n is even, and M can be written as the sum of $\frac{n}{2}$ mutually orthogonal complete subspaces, each being free of rank 2 as a Λ-module.*

PROOF Let $\chi_1 \in M$ such that $Sp_G\chi_1 \neq 0$, and let χ_2 be such that $\Phi(Sp_G\chi_1, \chi_2) = 1$. Then χ_1 and χ_2 generate a complete subspace of M, free of rank 2. Indeed, since $\Phi(Sp_G\chi_1, \chi_2) = \Phi(\chi_1, Sp_G\chi_2) \neq 0$, χ_2 must generate a free Λ-module; if $\lambda_1\chi_1 = \lambda_2\chi_2$ for some $\lambda_i \in \Lambda$, then $Sp_G\chi_1 = bSp_G\chi_2$ for some $b \in \mathbb{F}_p^\times$, and this would contradict lemma 1.4. If $\chi = \lambda_1\chi_1 + \lambda_2\chi_2 \in M$, and (without loss of generality) $t = ord_\pi(\lambda_1) \leq ord_\pi(\lambda_2)$, then $\Phi(\pi^{q-t-1}\chi_2, \chi) \neq 0$. Let $M_1 = \Lambda\chi_1 \oplus \Lambda\chi_2$, so that $M = M_1 \oplus M_1^\perp$ as complete spaces, with $M_1^\perp$ free of rank $n - 2$. The proposition follows by induction.◇

Proposition 1.2. *(i) A free rank two Λ-module M with nondegenerate, anti-symmetric form Φ possesses a splitting into two (necessarily free) totally isotropic subspaces.*

(ii) Such a "hyperbolic plane" is unique up to isometry. Precisely, there exist generators χ_1 and χ_2 of M such that the $\Lambda\chi_i$ are totally isotropic submodules, and such that,

$$\Phi(\chi_1, \sigma^i\chi_2) = \begin{cases} 1, & \text{if } i = 0, \\ 0, & \text{otherwise.} \end{cases} \tag{1.3}$$

6

PROOF As in the proof of proposition 1.1, let χ_1 and χ_2 generate M, with $\Phi(Sp_G\chi_1, \chi_2) = 1$. Notice first that the spaces $\mathcal{M}^{\frac{q-1}{2}}\chi_i$ are totally isotropic, since for $\lambda_i \in \mathcal{M}^{\frac{q-1}{2}}$,

$$\Phi(\lambda_1\chi_1, \lambda_2\chi_1) = \begin{cases} \Phi(\chi_1, uSp_G\chi_1), & \text{if } ord_\pi(\lambda_1) = ord_\pi(\lambda_2) = \frac{q-1}{2}; \\ 0, & \text{otherwise.} \end{cases}$$

Assume that we have found generators χ_1, χ_2 so that $\Phi(Sp_G\chi_1, \chi_2) = 1$ and so that $\mathcal{M}^t\chi_1$ and $\mathcal{M}^t\chi_2$ are totally isotropic subspaces of M, with $t \leq \frac{q-1}{2}$. If $\mathcal{M}^{t-1}\chi_1$ is not totally isotropic, then for some $\lambda_1, \lambda_2 \in \mathcal{M}^{t-1}$, we have $\Phi(\lambda_1\chi_1, \lambda_2\chi_1) = 1$. Since $\{\pi^j\chi_1, j = t-1, \ldots, q-1\}$ gives a basis of $\mathcal{M}^{t-1}\chi_1$, an easy calculation shows that $\Phi(\pi^{t-1}\chi_1, \pi^t\chi_1) = \epsilon \neq 0$. Let $\chi_1' = \chi_1 + \epsilon_0\pi^{q-2t}\chi_2$, with ϵ_0 to be chosen later. For $\lambda_i \in \Lambda$, we have

$$\begin{aligned} \Phi(\lambda_1\chi_1', \lambda_2\chi_1') &= \Phi(\lambda_1\chi_1 + \lambda_1\epsilon_0\pi^{q-2t}\chi_2, \lambda_2\chi_1 + \lambda_2\epsilon_0\pi^{q-2t}\chi_2) \\ &= \Phi(\lambda_1\chi_1, \lambda_2\chi_1) + \Phi(\lambda_1\epsilon_0\pi^{q-2t}\chi_2, \lambda_2\epsilon_0\pi^{q-2t}\chi_2) \\ &\quad + \Phi(\chi_1, (\lambda_1^*\lambda_2\epsilon_0\pi^{q-2t} - \lambda_2^*\lambda_1\epsilon_0\pi^{q-2t})\chi_2). \end{aligned}$$

If the λ_i are in $\mathcal{M}^t$, this expression is easily seen to be 0, while

$$\begin{aligned}\Phi(\pi^{t-1}\chi_1', \pi^t\chi_1') &= \Phi(\pi^{t-1}\chi_1, \pi^t\chi_1) + \Phi(\chi_1, \pi^{*t-1}\pi^{t-1}(\pi - \pi^*)\epsilon_0\pi^{q-2t}\chi_2) \\ &= \epsilon + \Phi(\chi_1, \epsilon_1\epsilon_0 Sp_G\chi_2).\end{aligned} \tag{1.4}$$

Here $\epsilon_1 \in \mathbb{F}_p$ is defined by $\pi^{*t-1}\pi^{t-1}(\pi - \pi^*)\pi^{q-2t} = \epsilon_1 Sp_G$. Thus if we take $\epsilon_0 = -\epsilon_1^{-1}\epsilon$, then $\mathcal{M}^{t-1}\chi_1'$ is totally isotropic, and $Sp_G\chi_1' = Sp_G\chi_1$. We can apply the same procedure to χ_2, producing a χ_2' such that $\mathcal{M}^{t-1}\chi_2'$ is totally isotropic, with $\Phi(Sp_g\chi_1', \chi_2') = 1$. This proves (i).

Suppose that Φ has the hyperbolic decomposition $M = \Lambda\chi_1 \oplus \Lambda\chi_2$ and Ψ has the hyperbolic decomposition $M = \Lambda\psi_1 \oplus \Lambda\psi_2$. The mapping $\alpha \colon \psi_i \mapsto \chi_i$ extends uniquely to a Λ-isomorphism of M onto itself, and we can define the form Ψ' on M by

$$\Psi'(x, y) = \Psi(\alpha^{-1}(x), \alpha^{-1}(y)).$$

Ψ and Ψ' are isometric forms. On the other hand, Ψ' has the hyperbolic decomposition $\Lambda\chi_1 \oplus \Lambda\chi_2$, and so by lemma 1.2, Φ and Ψ' are isometric. It follows that all forms having the properties of *(i)* are isometric. Defining Φ by (1.3) and extending by G-invariance, anti-symmetry, and total isotropy of the submodules $\Lambda\chi_i$ gives one representative of this isometry class.◇

Corollary. *A free Λ-module M with an anti-symmetric, nondegenerate, G-invariant form Φ possesses a decomposition into two totally isotropic subspaces; the isometry class of Φ is determined completely by the rank of M.*

PROOF This follows from propositions 1.1 and 1.2.◇

§ 1.3 In this section we examine the situation with $p = 2$. Thus $G = G_m$ is a cyclic group of order $q = 2^m$ with generator σ, Λ is the group ring $\mathbb{F}_2[G]$, and let M be a free Λ-module of rank n, possessing an anti-symmetric (and hence, symmetric) nondegenerate, G-invariant form $\Phi \colon M \times M \to \mathbb{F}_2$. Such a triple $\{M, \Phi, G\}$ will sometimes be called a symplectic space.

There are two complications arising in this situation which didn't appear for odd primes. The first problem is that now the form need not be alternating—not every vector need be isotropic. The second problem is that the result of lemma 1.4 need not hold. Following Koch [Ko 3], we will call Φ a "trace-form" if it satisfies the condition,

$$\Phi(\chi,\chi) = \Phi(\chi, Sp_G\chi) \quad \text{for all } \chi \in M. \tag{1.5}$$

This trace condition is equivalent to the condition (see [D 1]) that for all $\chi \in M$, $\Phi(\chi, \sigma^{\frac{g}{2}}\chi) = 0$. Indeed, since

$$\Phi(\chi, \sigma^i\chi) = \Phi(\sigma^{-i}\chi, \chi) = \Phi(\chi, \sigma^{-i}\chi)$$

for $i = 1, \ldots, \frac{g}{2} - 1$, we have $\Phi(\chi, (\sigma^i + \sigma^{-i})\chi) = 0$, and hence

$$\Phi(\chi, Sp_G\chi) = \Phi(\chi, (1 + \sigma^{\frac{g}{2}})\chi).$$

Proposition 1.3. *Suppose that the form Φ is alternating and satisfies the trace condition(1.5). Then*

(i) The rank n of M is even, and M decomposes into a sum of $\frac{n}{2}$ mutually orthogonal simple complete spaces of Λ-rank two;

(ii) In a decomposition given as in (i) above, each of the rank two submodules ("hyperbolic planes") possesses a splitting into two totally isotropic submodules;

(iii) The restriction of Φ to a hyperbolic plane is unique up to isometry;

(iv) M possesses a splitting into two totally isotropic submodules.

PROOF Assuming the trace condition, (i) follows by repeating the proof of proposition 1.1 *verbatim et kitteratim*. For (ii), one follows the idea of the proof of proposition 1.2 *mutatis mutandis*: let χ_1 and χ_2 generate the rank two Λ-module A, with

$$\Phi(\chi_1, Sp_G\chi_2) = 1. \tag{1.6}$$

It is clear that the subspaces $\mathcal{M}^{\frac{g}{2}}\chi_i$ are totally isotropic; the trace condition now shows that $\mathcal{M}^{\frac{g}{2}-1}\chi_i$ are totally isotropic. Now assume that generators χ_i satisfying (1.6) have been found such that $\mathcal{M}^t\chi_i$ are totally isotropic, with $t \leq \frac{g}{2} - 1$. By changing the χ_i if necessary with $\chi_1' = \chi_1 + \pi^{e-2t-1}\chi_2$ and

$\chi_2' = \chi_2 + \pi^{q-2t-1}\chi_1$, we obtain generators χ_i' satisfying (1.6) with $\mathcal{M}^{t-1}\chi_i'$ totally isotropic subspaces. For example,

$$\Phi(\pi^r\chi_1', \pi^s\chi_1') = \Phi(\pi^r\chi_1, \pi^s\chi_1) + \Phi(\pi^{q+r-2t-1}\chi_2, \pi^{q+s-2t-1}\chi_2) + \Phi(\chi_1, (\pi^{*r}\pi^{q+s-2t-1} + \pi^{*s}\pi^{q+r-2t-1})\chi_2). \tag{1.7}$$

By induction, and using the fact that the form is alternating, we need only check the case $r = t$, $s = t-1$. The second term of the right-hand-side of (1.7) becomes

$$\Phi(\pi^{q-t-1}\chi_2, \pi^{q-t-2}\chi_2) = \Phi(\chi_2, Sp_G\chi_2) = 0,$$

while the third term of (1.7) is

$$\Phi(\chi_1, \pi^{*t-1}\pi^{q-t-2}(\pi + \pi^*)\chi_2) = \Phi(\chi_1, Sp_G\chi_2) = 1,$$

since $\pi + \pi^* = \sigma x^2$. Thus, if $\mathcal{M}^{t-1}\chi_i$ is not isotropic, $\mathcal{M}^{t-1}\chi_i'$ will be. Proceeding in this way, we obtain (ii). The proof of (iii) is the same as the proof of proposition 1.2(ii)—one merely needs the existence of a hyperbolic decomposition; (iv) follows from (i) and (ii).◇

Suppose now that Φ is alternating and does not satisfy the trace condition (1.5) on the free Λ-module M. Define the operator

$$B_0 : M \to \mathbb{F}_2, \quad B_0(\chi) = \Phi(\chi, Sp_G\chi).$$

It's easy to see that $B_0 \in \mathrm{Hom}(\mathbf{M}, \mathbb{F}_2)$, and is non-trivial by assumption, so the non-degeneracy of Φ allows us to represent B_0 by a unique element $\theta_0 \in M$:

$$B_0(\chi) = \Phi(\theta_0, \chi) \quad \text{for all } \chi \in M.$$

Since B_0 is fixed under the action of G, θ_0 must also be fixed by G, and hence there is a ϕ such that $Sp_G\phi = \theta_0$. If $B_0(\phi) = 1$, then $\Lambda\phi = M_0$ is a complete subspace of M, and we may write

$$M = (\Lambda\phi) \oplus (\Lambda\phi)^{\perp} = M_0 \oplus M_1,$$

with the trace condition necessarily holding for the restriction of Φ to M_1.

If $B_0(\phi) = 0$, then we may find a ϕ_1 with $B_0(\phi_1) = \Phi(\theta_0, \phi_1) = 1$, and as in the proof of proposition 1.1, $\Lambda\phi \oplus \Lambda\phi_1$ is a complete subspace M_0 of M of rank two. Further, since

$$B_0(\phi_1) = \Phi(\phi_1, Sp_G\phi_1) = 1,$$

$\Lambda\phi_1$ is a complete subspace of M_0, so that M_0 decomposes as a sum of two complete rank one subspaces, the form on each of which is alternating and not satisfing the trace condition. The restriction of Φ to the orthogonal complement of M_0 is alternating and does satisfy the trace condition.

Suppose now that Φ is non-alternating on M and does satisfy the trace condition. As above, define

$$C_0 : M \to \mathbf{F}_2, \quad C_0(\chi) = \Phi(\chi, \chi) = \Phi(\chi, Sp_G\chi),$$

and represent $C_0 \in \mathrm{Hom}(M, \mathbf{F}_2)$ by the unique element ϱ_0:

$$C_0(\chi) = \Phi(\varrho_0, \chi) \quad \text{for all } \chi \in M.$$

Again, C_0, and hence ϱ_0, is fixed by G, so there is a ϱ with $Sp_G\varrho = \varrho_0$. If $C_0(\varrho) = 1$, then $\Lambda\varrho$ is a complete subspace of M, and the restriction of Φ to the orthogonal complement of $\Lambda\varrho$ is alternating and satisfies the trace condition. If, on the other hand, $C_0(\varrho) = 0$, then for any ν with $C_0(\nu) = \Phi(\varrho_0, \nu) = 1$, the subspace $\Lambda\varrho \oplus \Lambda\nu = M_0$ is complete, and the restriction of Φ to $M_0^\perp$ is alternating and satisfies the trace condition. Furthermore, since $\Phi(\nu, Sp_G\nu) = 1$, $\Lambda\nu$ is complete, and M_0 decomposes as the sum of two complete rank one subspaces, on each of which the form is a non-alternating trace form.

Finally, suppose that the form Φ on M is non-alternating and is not a trace-form. As above, let $C_0(\chi) = \Phi(\chi, \chi)$, and represent C_0 by the G-norm ϱ_0, with $Sp_G\varrho = \varrho_0$. If $C_0(\varrho) = 1$, then $\Lambda\varrho$ is a complete subspace M_0 of M (on which the restriction of Φ is a trace-form), and the restriction of Φ to $M_0^\perp$ is alternating and doesn't satisfy the trace condition. If $C_0(\varrho) = 0$, choose η with

$$C_0(\eta) = \Phi(\eta, \eta) = \Phi(\eta, \varrho_0) = 1$$

so that $M_0 = \Lambda\eta \oplus \Lambda\varrho$ is a complete subspace of M, and the restriction of Φ to $M_0^\perp$ is alternating—Φ may or may not be a trace form on $M_0^\perp$, but either case is treated above. On M_0, the form is a trace-form if and only if $\Phi(\eta,\eta) = \Phi(\eta, S_{PG}\eta) = 1$; if this occurs, then M_0 decomposes into two complete rank one subspaces with the trace condition holding.

If the trace condition doesn't hold on M_0, then $\Phi(\eta, S_{PG}\eta) = 0$, and M_0 is necessarily simple. We now show that this rank two space is unique up to isometry. First note that Φ is alternating on πM_0, since $\Phi(\pi\chi, \pi\chi) = \Phi(\pi\chi, S_{PG}\varrho) = 0$. Assume that we have found η and ϱ so that $\mathcal{M}^t\eta$ and $\mathcal{M}^t\varrho$ are totally isotropic subspaces, with $t \geq 2$. If $\mathcal{M}^{t-1}\varrho$ and $\mathcal{M}^{t-1}\eta$ are not totally isotropic, the same calculation as (1.7) shows that we can find η' and ϱ' so that $S_{PG}\varrho' = S_{PG}\varrho$, $\Phi(\eta', S_{PG}\varrho') = 1$, and $\mathcal{M}^{t-1}\varrho'$ and $\mathcal{M}^{t-1}\eta'$ are totally isotropic. Proceeding inductively, we thus can find η and ϱ so that Φ is totally isotropic on the subspaces $\mathcal{M}\eta$ and $\mathcal{M}\varrho$. Now $\Phi(\varrho, \varrho) = 0$, so that we may apply the above procedure one more time if necessary to ϱ to insure that $\Lambda\varrho$ is totally isotropic. The story is different with η: we can, if necessary, change η to $\eta' = \eta + \pi^{q-2}\varrho$ so that both $\Phi(\eta', \pi\eta') = 0$ holds, and $\mathcal{M}\eta'$ is istropic. Thus the values of Φ on $\Lambda\eta$ and on $\Lambda\varrho$ are determined.

We now show that ϱ can be chosen so that

$$\Phi(\eta, \pi^i\varrho) = 1, \tag{1.8}$$

for all $i \leq q-1$. Indeed, having found ϱ so that (1.8) holds for $t \leq i \leq q-1$, suppose that $\Phi(\eta, \pi^{t-1}\varrho) = 0$. Letting $\varrho' = \varrho + \pi^{q-t}\varrho$, we obtain (1.8) for $t-1 \leq i \leq q-1$, and proceeding inductively, we obtain (1.8) for all $i \leq q-1$. Since this process amounted merely to finding a new generator for the totally isotropic subspace $\Lambda\varrho$, the values of Φ on the subspaces $\Lambda\varrho$ and $\Lambda\eta$ are unchanged. We recapitulate the above results in the following proposition.

Proposition 1.4. *Let M be a free Λ-module of rank n with the anti-symmetric, G-invariant, nondegenerate form Φ. Then M is one of the following types:*

(1) Φ is alternating and satisfies the trace condition (1.5). Then n is even, and M can be written as a sum of $\frac{n}{2}$ simple hyperbolic planes; there is, up to isometry, only one class of form on each of these planes.

(2) Φ is non-alternating and satisfies the trace condition. If n is odd, then M decomposes as the sum of a simple rank-one subspace on which the form is non-alternating, and a complete subspace of rank $n - 1$

on which the form is of type (1). If the rank is even, then M decomposes as the sum of two simple rank one subspaces (on each of which the form is non-alternating) and a complete subspace of rank $n-2$ of type (1).

(3) Φ is alternating and does not satisfy the trace condition. If n is odd, then M decomposes as the sum of a simple subspace of rank one (on which the form is alternating and without the trace condition), and a complete subspace of rank $n-1$ of type (1). If n is even, then M decomposes as the sum of two simple rank one subspaces (on each of which the form is alternating and without the trace condition) and a subspace of rank $n-2$ of type (1).

(4) Φ is non-alternating and without the trace condition. There is only one class of simple space of this type, having rank two. If n is even then either: M decomposes as the sum of this simple of rank two and a subspace of type (1) of rank $n-2$; or as the sum of a simple of this type and a subspace of type (3) of even rank; or as the sum of a simple subspace of type (2), a simple subspace of type (3), and a subspace of type (1) of rank $n-2$; or as the sum of two simples of type (2), two simples of type (3), and a complete subspace of rank $n-4$ of type (1). If n is odd, then we can decompose M in one of two ways: either as a sum of two simples of type (2), a simple of type (3), and a rank $n-3$ subspace of type (1); or as a sum of two simples of type (3), a simple of type (2), and a rank $n-3$ subspace of type (1).

PROOF All has been proved except the decompositions given in (4). Since Φ is non-alternating, we can represent the homomorphism $\chi \mapsto \Phi(\chi,\chi)$ by a non-trivial G-norm $\nu_0 = Sp_G\nu$ in M. If $\Phi(\nu,\nu) = \Phi(\nu, Sp_G\nu) = 1$, then $\Lambda\nu$ is complete, and it's orthogonal complement is of type (3) (if the trace condition were satisfied on both components, it would be satisfied on the whole). If $\Phi(\nu,\nu) = 0$, find η so that $\Phi(\eta,\eta) = \Phi(\eta, Sp_G\nu) = 1$. Then $M_0 = \Lambda\eta + \Lambda\nu$ is complete, and we can write $M = M_0 \oplus M_0^\perp$, with the form on $M_0^\perp$ alternating. If the form satisfies the trace condition on M_0, then it cannot be a trace-form on $M_0^\perp$, and $M_0^\perp$ is of type (3); if we do not have a trace form on M_0, then M_0 is a simple subspace of type (4), and the complement $M_0^\perp$ may or may not have the trace condition, being either of type (1) or of type (3).◇

Remark. Note that if one takes the sum of a simple of type (4) with a simple of type (2), the resulting space can be decomposed as the sum of a simple of type (2) and two simples of type (3).

§ 1.4 We preserve the notations and conventions of the previous section. In order to complete the classification of symplectic forms on M, we will need to know the isometry classes of those symplectic forms which can occur on rank-one Λ-modules.

Define the group ring "trace"

$$\ell\colon \Lambda \to \mathbb{F}_2, \quad \ell\Big(\sum_{i=0}^{q-1} a_i\sigma^i\Big) = a_0.$$

Given any $d \in \Lambda$, we can define a pairing $\Phi_d\colon \Lambda \times \Lambda \to \mathbb{F}_2$ by

$$\Phi_d(\lambda, \mu) = \ell(\lambda d \mu^*)$$

which is $\mathbb{F}_2$-bilinear and G-invariant. Conversely, given any G-invariant form Φ on the free Λ-module $\Lambda\chi$, let $d_\Phi = \sum_{i=0}^{q-1} d_i\sigma^i$ be given by $d_i = \Phi(\chi, \sigma^i\chi)$.

Lemma 1.5. *(i) The correspondence $\Phi \leftrightarrow d_\Phi$ gives a bijection between G-invariant forms on a free rank one Λ-module and elements of Λ;*

(ii) The form Φ_d is nondegenerate if and only if $d \in \Lambda^\times$;

(iii) Φ_d is symmetric if and only if $d^* = d$;

(iv) The forms Φ_d and $\Phi_{d'}$ are isometric if and only if there is a unit $u \in \Lambda^\times$ with $d' = udu^*$;

(v) If Φ_d is nondegenerate, then Φ_d is a trace form if and only if $\ell(d) = 1$.

PROOF The values of the form Φ are determined by its values on the basis $\chi, \sigma\chi, \ldots, \sigma^{q-1}\chi$, and the G-invariance of the form means we need only check the values $\Phi(\chi, \sigma^i\chi)$—these are precisely the same as the values $\Phi_{d_\Phi}(1, \sigma^i)$. Since two different d's will give different forms, we have (i). If λ is in the radical of the form Φ_d, then $\ell(\lambda d\sigma^{-i}) = 0$ for all $0 \le i \le q-1$, so that $\lambda d = 0$, and d is a non-unit, and conversely. This proves (ii). The form Φ_d is symmetric if and only if $\ell(\sigma d) = \ell(d\sigma^{-i})$ for all i, so that $d_i = d_{q-i}$ and

d is fixed by the involution '$*$', hence (iii). A Λ-automorphism of Λ is given by (right-) multiplication by some unit $u \in \Lambda^{\times}$. Thus, the forms Φ_d and $\Phi_{d'}$ are isometric if there is a unit u such that

$$\Phi_{d'}(\lambda, \mu) = \Phi_d(\lambda u, \mu u)$$

for all λ and μ in Λ. Hence, with $\lambda = 1$ and $\mu = \sigma^i$, we have

$$\ell(d'\sigma^{-i}) = \ell(udu^*\sigma^{-i})$$

for all i, and thus $d' = udu^*$. Finally, if Φ_d is a trace form, then $\Phi_d(1,1) = \Phi_d(Sp_G, 1)$, and hence $\ell(d) = \ell(Sp_G d) = 1$ for d a unit. For the converse, one checks that if $\ell(d) = 1$, then

$$\Phi_d(\sigma^i, \sigma^i) = \Phi_d(\sigma^i, Sp_G\sigma^i) = 1$$

for d a unit.◇

Corollary. *The isometry classes of symmetric, nondegenerate, G-invariant forms on a free rank-one Λ-module are in one to one correspondence with the equivalence classes of elements of $\Lambda^{\times}$, where two such elements d and d' are said to be equivalent if there is a u such that $d' = udu^*$.*

Let Δ be a cyclic group generated by g, and let A be a Δ-module. Define the Tate cohomology groups (see [S 1], chapter VIII) to be the homology groups of the complex,

$$\ldots \rightarrow A \xrightarrow{Sp_\Delta} A \xrightarrow{1-g} A \xrightarrow{Sp_\Delta} A \rightarrow \ldots$$

$$\hat{H}^0(\Delta, A) = \frac{\ker(1-g)}{\operatorname{im}(Sp_\Delta)} = \frac{A^\Delta}{Sp_\Delta A}$$

$$\hat{H}^1(\Delta, A) = \frac{\ker(Sp_\Delta)}{\operatorname{im}(1-g)}$$

The above corollary thus says that the isometry classes in question are in one-to-one correspondence with the elements of the cohomology group $\hat{H}^0(\Delta, \Lambda^{\times})$, where Δ is the group $\{1, *\}$.

We can compute the $\hat{H}^i(\Delta, \Lambda_2^{\times})$ by hand, where we're letting $\Lambda_m = \mathbf{F}_2[G_m]$:

$$\Lambda_2^{\times} = \{1, \sigma, \sigma^2, \sigma^3, 1+\sigma+\sigma^2, 1+\sigma+\sigma^3, 1+\sigma^2+\sigma^3, \sigma+\sigma^2+\sigma^3\},$$

$$\ker(1-*) = \{1, \sigma^2, 1+\sigma+\sigma^3, \sigma+\sigma^2+\sigma^3\},$$

$$\mathrm{im}(1+*) = \{1\}; \quad \mathrm{im}(1-*) = \{1,\sigma^2\}; \quad \ker(1+*) = \Lambda^\times.$$

We thus obtain that

$$\hat{H}^0(\Delta, \Lambda_2^\times) \cong \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/2\mathbf{Z},$$

generated by the classes of σ^2 and $1+\sigma+\sigma^3$; and that

$$\hat{H}^1(\Delta, \Lambda_2^\times) \cong \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/2\mathbf{Z},$$

generated by the classes of σ and $1+\sigma+\sigma^3$. As an aid to computing $\hat{H}^i(\Delta, \Lambda_m^\times)$, we first compute the cohomology of the *additive* group Λ_m for $q = 2^m \geq 4$.

Lemma 1.6. *$\hat{H}^0(\Delta, \Lambda) \cong \hat{H}^1(\Delta, \Lambda) \cong \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/2\mathbf{Z}$, generated by the classes of* 1 *and* $\sigma^{\frac{q}{2}}$.

PROOF In this case, the operators $1-*$ and $1+*$ are the same, so the cohomology groups are isomorphic. Now the Δ-fixed elements of Λ have the basis $\{1, \sigma+\sigma^{-1}, \ldots, \sigma^{\frac{q}{2}-1}+\sigma^{\frac{q}{2}+1}, \sigma^{\frac{q}{2}}\}$; the subspace of norms is precisely the subspace generated by the $(1+*)\sigma^i = \sigma^i + \sigma^{-i}$.◇

Lemma 1.7. *For all $m \geq 2$, one has*

$$\hat{H}^0(\Delta, \Lambda_m^\times) \cong \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/2\mathbf{Z},$$

generated by the classes of $\sigma^{2^{m-1}}$ and $1+\sigma+\sigma^{-1}$; and

$$\hat{H}^1(\Delta, \Lambda_m^\times) \cong \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/2\mathbf{Z},$$

generated by the classes of σ and $1+\sigma^{2^{m-2}}+\sigma^{-2^{m-2}}$.

PROOF We proceed by induction, the case $m = 2$ having been already proved above. The surjection of groups $G_m \to G_{m-1}$ induces the surjective ring homomorphism $\beta: \Lambda_m \to \Lambda_{m-1}$, and hence one has the exact sequence of groups:

$$1 \longrightarrow K_m \xrightarrow{\iota} \Lambda_m^\times \xrightarrow{\beta} \Lambda_{m-1}^\times \longrightarrow 1\,, \tag{1.9}$$

where $K_m = 1 + M^{2^{m-1}}$ is the subgroup of $\Lambda_m^\times$ of elements of order 2. It's easy to see that (1.9) is an exact sequence of Δ-modules, and thus gives rise to the following "exact hexagon" ([S 1],VIII§4),

$$\begin{tikzcd}
 & \hat{H}^0(\Delta, K_m) \arrow[r, "\iota^0"] & \hat{H}^0(\Delta, \Lambda_m^\times) \arrow[dr, "\beta^0"] & \\
\hat{H}^1(\Delta, \Lambda_{m-1}^\times) \arrow[ur, "\delta^1"] & & & \hat{H}^0(\Delta, \Lambda_{m-1}^\times) \arrow[dl, "\delta^0"] \\
 & \hat{H}^1(\Delta, \Lambda_m^\times) \arrow[ul, "\beta^1"] & \hat{H}^1(\Delta, K_m) \arrow[l, "\iota^1"'] &
\end{tikzcd} \tag{1.10}$$

We can identify K_m and Λ_{m-1}^+ as Δ-modules by the map,

$$\phi: \Lambda_{m-1} \to K_m, \quad \bar{x} \mapsto 1 + (1 + \sigma^{2^{m-1}})x,$$

where $x \in \Lambda_m$ is any lifting under β of $\bar{x} \in \Lambda_{m-1}$ (any two such liftings will differ by an element of $\mathcal{M}^{2^{m-1}}$, so ϕ is well-defined). Using lemma 1.6, it follows that

$$\hat{H}^0(\Delta, K_m) \cong \hat{H}^1(\Delta, K_m) \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z},$$

generated by the classes of the elements $1 + (1 + \sigma^{2^{m-1}})(1) = \sigma^{2^{m-1}}$ and $1 + (1 + \sigma^{2^{m-1}})(\sigma^{2^{m-2}}) = 1 + \sigma^{2^{m-2}} + \sigma^{3 \cdot 2^{m-2}}$.

We must compute the connecting homomorphisms (using the "snake-lemma"): if $\bar{x} \in \ker(\Lambda_{m-1}^\times \xrightarrow{1-*} \Lambda_{m-1}^\times)$, then $\delta^0(\bar{x})$ is (the class of) the element $x(x^*)^{-1}$, where x is any lifting of $\bar{x}$ in $\Lambda_m^\times$. By induction, we find that image of δ^0 is generated by the class of

$$\delta^0(\overline{\sigma^{2^{m-2}}}) = \sigma^{2^{m-2}}(\sigma^{2^{m-2}*})^{-1} = \sigma^{2^{m-1}},$$

and by the class of $\delta^0(1 + \bar{\sigma} + \overline{\sigma^{-1}}) = 1$.

If now $\bar{x} \in \ker(\Lambda_{m-1}^\times \xrightarrow{1+*} \Lambda_{m-1})$, then $\delta^1(\bar{x})$ is the class of the element xx^* in $\hat{H}^0(\Delta, K_m)$. Thus the image of δ^1 is generated by the classes of $\delta^1(\bar{\sigma}) = 1$ and

$$\begin{aligned} \delta^1(1 + \overline{\sigma^{2^{m-2}}} + \overline{\sigma^{-2^{m-2}}}) &= (1 + \sigma^{2^{m-2}} + \sigma^{-2^{m-2}})(1 + \sigma^{2^{m-2}*} + \sigma^{-2^{m-2}*}) \\ &= 1 + \sigma^{2^{m-2}} + \sigma^{3 \cdot 2^{m-2}}. \end{aligned}$$

The exactness of (1.10) now shows that $\hat{H}^0(\Delta, \Lambda_m^\times)$ must be generated by the image of $\sigma^{2^{m-1}}$ under ι^0 and by a pre-image of $1 + \bar{\sigma} + \overline{\sigma^{-1}}$, hence by (the classes of) $\sigma^{2^{m-1}}$ and $1 + \sigma + \sigma^{-1}$; $\hat{H}^1(\Delta, \Lambda_m^\times)$ will be generated by $\iota^1(1 + \sigma^{2^{m-2}} + \sigma^{3 \cdot 2^{m-2}})$ and by a pre-image of $\bar{\sigma}$, hence by σ and $1 + \sigma^{2^{m-2}} + \sigma^{-2^{m-2}}$.◇

Corollary. *Let $m \geq 2$. A free, rank-one Λ-module possesses four distinct isometry classes of nondegenerate symplectic forms. There are two classes of non-alternating trace-forms, given by the representatives 1 and $1 + \sigma + \sigma^{-1}$; and there are two classes of alternating, non-trace-forms, given by the representatives $\sigma^{2^{m-1}}$ and $\sigma^{2^{m-1}} + \sigma^{2^{m-1}+1} + \sigma^{2^{m-1}-1}$.*

Lemma 1.8. *Let Φ be a non-alternating trace-form on the free Λ-module M, and let ϱ_0 represent the homomorphism $\chi \to \Phi(\chi, \chi)$. If $\varrho \in M$ with $Sp_G \varrho = \varrho_0$, then*

$$\Phi(\varrho, \pi^{q-3} \varrho) = \iota_M \tag{1.11}$$

is an invariant of the symplectic space M.

PROOF If $Sp_G \varrho' = \varrho_0$, then $\varrho' = \varrho + \pi\gamma$ for some $\gamma \in M$, and

$$\begin{aligned} \Phi(\varrho', \pi^{q-3}\varrho') &= \Phi(\varrho, \pi^{q-3}\varrho) + \Phi(\pi\gamma, \pi^{q-3}\varrho) + \Phi(\varrho, \pi^{q-2}\gamma) + \Phi(\pi\gamma, \pi^{q-2}\gamma) \\ &= \iota_M + \Phi(\pi\pi^{*q-3}\gamma + \pi^{q-2}\gamma, \varrho) + \Phi(\gamma, Sp_G\gamma) \qquad (1.12) \\ &= \iota_M + \Phi(\pi(\pi^{*q-3} + \pi^{q-3})\gamma, \varrho) + \Phi(\gamma, \varrho_0). \end{aligned}$$

Now $\pi(\pi^{q-3} + \pi^{*q-3}) = Sp_G$: indeed, one has,

$$\pi^{q-3} = 1 + \sigma + \sigma^4 + \sigma^5 + \ldots + \sigma^{4h} + \sigma^{4h+1} + \ldots + \sigma^{q-4} + \sigma^{q-3}, \tag{1.13}$$

as may be verified by multiplying both sides of the identity

$$X^{q-3} = 1 + (1 + X) + \ldots + (1 + X)^{q-3}$$

in $\mathbb{F}_2[X]$ by $(1 + X)^2$ and reducing mod X^q. Applying the involution $*$ to equation (1.13) gives

$$\pi^{*q-3} = 1 + \sigma^{q-1} + \sigma^{q-4} + \sigma^{q-5} + \ldots + \sigma^4 + \sigma^3. \tag{1.14}$$

Inspection shows that

$$\pi^{q-3} + \pi^{*q-3} = \sigma + \sigma^3 + \sigma^5 + \ldots + \sigma^{q-1},$$

and multiplying this equation by π proves the claim. Finally,

$$\Phi(Sp_G\gamma, \varrho) = \Phi(\gamma, Sp_G\varrho) = \Phi(\gamma, \varrho_0),$$

which, when substituted into calculation (1.12), shows that ι_M is independent of the choice of ϱ.◇

We call ι_M the "Koch invariant*" of the form Φ.

[*] Koch's original invariant, defined in [Ko 3], is of the opposite parity.

Lemma 1.9. *The Koch invariant distinguishes between the two non-alternating trace-forms on a free rank-one* Λ*-module* M.

PROOF Let $\Lambda\varrho = M$; by the corollary to lemma 1.7, the generator ϱ may be chosen so that

$$\Phi(\lambda\varrho, \mu\varrho) = \begin{cases} \ell(\lambda(1+\sigma+\sigma^{-1})\mu^*), & \text{"case 1,"} \\ \ell(\lambda(1)\mu^*), & \text{"case 2."} \end{cases}$$

In case 1, we have from equation (1.14),

$$\iota_M = \ell((1+\sigma+\sigma^{-1})(1+\sigma^{q-1}+\ldots+\sigma^3)) = 0,$$

while in case 2,

$$\iota_M = \ell(1+\sigma^{q-1}+\ldots+\sigma^3) = 1. \quad \diamond$$

Lemma 1.10. *There are two isometry classes of non-alternating trace-forms on a free rank-two* Λ*-module* M*, distinguished by their Koch invariant.*

PROOF Let $M = \Lambda\chi_1 \oplus \Lambda\chi_2$ be a decomposition of M into simple spaces. Suppose first that the Koch invariant of the restriction of Φ to each of these subspaces is 1—that is, the χ_i can be chosen so that

$$\Phi(\lambda\chi_i, \mu\chi_i) = \ell(\lambda\mu^*).$$

Since $\varrho_0 = Sp_G(\chi_1+\chi_2)$, the Koch invariant of M is

$$\iota_M = \Phi(\chi_1+\chi_2, \pi^{q-3}(\chi_1+\chi_2)) = 1+1 = 0. \tag{1.15}$$

If we let

$$\chi_1' = \chi_1 + \pi\chi_2, \quad \chi_2' = \pi^*\chi_1 + \chi_2,$$

then $M = \Lambda\chi_1' \oplus \Lambda\chi_2'$ as symplectic spaces, and one can check that the Koch invariant of each of these spaces is 0. Hence two spaces M_1 and M_2, each the sum of two simples having the same Koch invariant, are isometric, and this is reflected by the fact that $\iota_{M_1} = \iota_{M_2} = 0$. If the Koch invariant of $\Lambda\chi_1$ is 1, and the Koch invariant of $\Lambda\chi_2$ is 0, then a calculation similar to (1.15) shows that $\iota_M = 1.\diamond$

Proposition 1.5. *The Koch invariant ι_M, together with the rank of the free* Λ*-module M, give a complete set of invariants for the isometry classes of non-alternating trace-forms* on M.

PROOF This follows immediatly from proposition 1.4 and lemmas 1.8–1.10. ◇

Though in the sequel we will be concerned only with trace-forms, we complete the classification of symplectic forms on free Λ-modules with the following proposition.

Proposition 1.6. *Let Φ be an alternating non-trace-form on the free* Λ*-module M, and let θ_0 represent the homomorphism $\chi \mapsto \Phi(\chi, Sp_G\chi)$. Let $Sp_G\theta = \theta_0$, and define*

$$\kappa_M = \Phi(\theta, \pi^{g-2}\theta).$$

Then κ_M is well-defined, and κ_M together with the rank of M form a complete set of invariants for the isometry class of Φ.

PROOF One repeats the proofs of lemmas 1.7–1.9 *mutatis mutandis*, to show that κ_M distinguishes classes of rank-one and rank-two spaces, and then applies proposition 1.4.◇

§ 1.5 In this section, G will denote an Abelian group with Sylow 2-subgroup G_2 cyclic of order q. Let H be the subgroup of G of elements of order prime to 2, so that $G = HG_2$, and let $\Lambda = \mathbb{F}_2[G]$. The object of this section is to classify nondegenerate, symmetric, G-invariant forms on a free Λ-module M of rank n.

We first decompose the $\mathbb{F}_2$-algebra Λ into its indecomposable constituants as follows: the sub-algebra $\mathbb{F}_2[H]$, being semisimple, decomposes as a direct sum of sub-algebras isomorphic to finite field extensions of $\mathbb{F}_2$,

$$\mathbb{F}_2[H] = \oplus_{i=1}^{r}\mathbb{F}_2[H]e_i \cong \oplus_i K_i, \tag{1.16}$$

where the e_i's are (uniquely defined) primitive orthogonal idempotents—in what follows we will identify $\mathbb{F}_2[H]e_i$ with K_i by means of a fixed isomorphism, and consider (when necessary) K_i as a (left) $\mathbb{F}_2[H]$-module by means of this identification. Of particular interest in the sequel is the idempotent,

$$E = e_1 = Sp_H = \sum_{h \in H} h,$$

which splits the augmentation map $\varepsilon: \mathbb{F}_2[H] \to \mathbb{F}_2$, so that $K_1 = \mathbb{F}_2$. All other K_i's are nontrivial extensions of $\mathbb{F}_2$.

The involution $*$ on Λ restricts to an (anti-) isomorphism of $\mathbb{F}_2[H]$ onto itself, sending primitive idempotents to primitive idempotents. Order the e_i's so that $e_1, \ldots, e_{r_1}$ are those idempotents fixed by $*$, and $e_{r_1+1}, e^*_{r_1+1}, \ldots, e_{r_1+r_2}, e^*_{r_1+r_2}$ are those idempotents interchanged in pairs. It follows that for $1 \leq i \leq r_1$, the involution restricts to an automorphism of the summand $\mathbb{F}_2[H]e_i$, and hence may be identified with a Galois automorphism $J = J_i$ of the field K_i. J_1 is certainly trivial, but for $2 \leq i \leq r_1$, J_i is the unique non-trivial galois automorphism of order 2. Indeed, let $h \in H$ have image $\xi \neq 1$ under the composition,

$$\mathbb{F}_2[H] \to \mathbb{F}_2[H]e_i \cong K_i.$$

Then $h^* = h^{-1}$ has image $\xi^J = \xi^{-1} \neq \xi$, so that J is nontrivial.

We now "adjoin" G_2, keeping in mind that the idempotents e_i remain central and mutually orthogonal:

$$\begin{aligned}\Lambda = \mathbb{F}_2[G] = \mathbb{F}_2[H.G_2] &= \mathbb{F}_2[H][G_2]\\ &= \oplus \mathbb{F}_2[H][G_2]e_i\\ &\cong \oplus K_i[G_2].\end{aligned}$$

This is a decomposition of Λ into indecomposables, since the summands $K_i[G_2]$ are local rings. Note that, for $1 \leq i \leq r_1$, the involution $*$ will restrict to an involution (also called $*$) on the summand $K_i[G_2]$,

$$\Big(\sum_{g \in G_2} \xi_g g\Big)^* = \sum_{g \in G_2} \xi_g^J g^{-1}.$$

Lemma 1.11. *Let R be a ring with involution $*$, and let Φ be a nondegenerate, R-invariant form on the left R-module M. Suppose that E_i are central, mutually orthogonal idempotents which are fixed by $*$, suppose $\sum E_i = 1$ in R, and let $R_i \cong R.E_i$. Then the form Φ restricts to a nondegenerate, R_i-invariant form Φ_i on the R-submodule $E_i.M = M_i$, and the isometry class of Φ is uniquely determined by the isometry classes of the Φ_i.*

PROOF If $x = E_i.x \in E_i.M$, and $\Phi(x,y) \neq 0$, then $\Phi(E_i.x, y) = \Phi(E_i.x, E_i.y) = \Phi_i(E_i.x, E_i.y) \neq 0$, so that the Φ_i are nondegenerate; if $\alpha: M \to M$ is an isometry of forms Φ and Ψ, then $\alpha(E_i.x) = E_i.\alpha(x)$, so that α restricts to an isometry α_i of forms Φ_i and Ψ_i on M_i. Conversely, given R_i-invariant forms Φ_i on M_i, we may construct an R-invariant form Φ on $M \cong \oplus M_i$ in the obvious way: namely, consider the M_i as R-modules by means of the surjection $R \to R.E_i \cong R_i$, so that the forms Φ_i become R-invariant forms; the form Φ is defined to be their sum (as R-invariant forms). A formal computation shows that R_i-isometries of forms Φ_i and Ψ_i will determine an R-isometry of the constructed forms Φ and Ψ.◇

We will apply this lemma with $R = \Lambda = \mathbb{F}_2[G]$, the idempotents being

$$E_i = \begin{cases} e_i, & \text{for } 1 \leq i \leq r_1, \\ e_i + e_i^*, & \text{for } r_1 + 1 \leq i \leq r_1 + r_2. \end{cases}$$

In view of the above lemma, if M is a free Λ-module, then the isometry classes of symmetric, nondegenerate, G-invariant forms on M are in one-to-one correspondance with sums of isometry classes of ΛE_i-invariant forms on the free ΛE_i-modules $E_i.M$.

§ 1.6 In this section, let k be a finite field extension of $\mathbb{F}_2$, let $J \in \mathrm{Ga}$[illegible] either trivial or of order 2, and let G_2 be a cyclic 2-group of order $q = 2^m$. Let R be the group ring $k[G_2]$, with involution $*$ defined by

$$(\sum_{g \in G_2} \xi_g . g)^* = \sum_{g \in G_2} \xi_g^J . g^{-1}. \tag{1.17}$$

If M is a free left R-module of rank n, a "sesquilinear form" Φ on M is a bi-additive pairing $M \times M \to R$ such that for all $r \in R$ and $m_1, m_2 \in M$ one has

$$\Phi(r.m_1, m_2) = r\Phi(m_1, m_2) = \Phi(m_1, r^*.m_2).$$

We will call such a form "Hermitian" if $\Phi(m_1, m_2) = \Phi(m_2, m_1)^*$, and Φ is said to be nondegenerate (on the left) if for any $m_1 \in M$ there is an m_2 such that $\Phi(m_1, m_2) \neq 0$. Two sesquilinear forms Φ and Ψ are said to be equivalent on M if there is a non-singular, R-linear transformation α of M such that for all $m_1, m_2 \in M$,

$$\Phi(\alpha(m_1), \alpha(m_2)) = \Psi(m_1, m_2).$$

Proposition 1.7. *There is a one-to-one correspondence between equivalence classes of (nondegenerate, Hermitian) sesquilinear forms on the free R-module M, and isometry classes of R-invariant forms* : $M \times M \to \mathbb{F}_2$.

PROOF Define (as in [FM 1], section 7) the "involution-trace" to be the composition

$$\ell \colon k[G_2] \xrightarrow{\ell_1} k \xrightarrow{Tr} \mathbb{F}_2,$$

where $\ell_1(\sum \xi_g . g) = \xi_1$ and Tr is the field trace from k to $\mathbb{F}_2$. ℓ satisfies the following properties:

1) ℓ is $\mathbb{F}_2$-linear;

2) $\ell(a^*) = \ell(a)$;

3) The pairing $L \colon R \times R \to \mathbb{F}_2$ given by

$$L(a_1, a_2) = \ell(a_1 a_2^*),$$

is non-singular.

Let $e_1,\ldots,e_t$ be a basis for R over $\mathbb{F}_2$, and let $f_1,\ldots,f_t$ be the dual basis with respect to the pairing in 3): $\ell(e_i f_j^*) = \delta_{i,j}$.

Given Φ a sesquilinear form on M, define

$$\Phi_*: M \times M \to \mathbb{F}_2, \quad \Phi_*(m_1,m_2) = \ell(\Phi(m_1,m_2)).$$

It is immediate from the definitions that Φ_* is an R-invariant form on M, and that equivalent sesquilinear forms give isometric R-invariant forms. It is also clear that if Φ is a Hermitian form, then Φ_* is symmetric. If Φ is nondegenerate, and $m_1 \in M$, there is an $m_2 \in M$ with $\Phi(m_1,m_2) = \lambda \in R$. Let $\mu \in R$ be such that $\ell(\lambda\mu^*) = 1$—this can be done by property 3) of ℓ—so that

$$\Phi_*(m_1,\mu m_2) = \ell(\Phi(m_1,\mu m_2)) = \ell(\mu^*\lambda) = 1,$$

and the form Φ_* is nondegenerate.

Conversely, suppose that Ψ is an R-invariant form on M, and define the pairing

$$\Psi^*(m_1,m_2) = \sum_{i=1}^{t} \Psi(m_1, f_i m_2) e_i \in R.$$

Then Ψ^* is sesquilinear: given $x \in R$, let

$$x\Psi^*(m_1,m_2) = \sum_{i=1}^{t} \lambda_i e_i,$$

$$\lambda_i = L(x\Psi^*(m_1,m_2), f_i) = \ell(x\Psi^*(m_1,m_2) f_i^*) \in \mathbb{F}_2.$$

But then,

$$\begin{aligned} \lambda_i &= \ell(x(\sum_{j=1}^{t} \Psi(m_1, f_j m_2) e_j) f_i^*) \\ &= \sum_j \ell(x\Psi(m_1, f_j m_2) e_j f_i^*) \\ &= \sum_j \ell(x e_j f_i^*)\Psi(m_1, f_j m_2)) \\ &= \Psi(m_1, \sum_j \ell(x e_j f_i^*) f_j m_2). \end{aligned} \tag{1.18}$$

The properties of ℓ show that $\ell(x e_j f_i^*) = \ell(x^* f_i e_j^*)$, and using the fact that the f_j's are a basis of R having the e_j's as dual basis (for the pairing L),

$$\sum_j \ell(x e_j f_i^*) f_j = \sum_j \ell(x^* f_i e_j^*) f_j = x^* f_i,$$

from which it follows that Ψ^* is sesquilinear.

Finally, the associations $\Phi \mapsto \Phi_*$ and $\Psi \mapsto \Psi^*$ are mutually inverse to each other:

$$\begin{aligned}(\Phi_*)^*(m_1, m_2) &= \sum_i \Phi_*(m_1, f_i m_2) e_i \\ &= \sum_i \ell(\Phi(m_1, f_i m_2)) e_i \\ &= \sum_i \ell(f_i^* \Phi(m_1, m_2)) e_i \\ &= \Phi(m_1, m_2);\end{aligned}$$

and

$$\begin{aligned}(\Psi^*)_*(m_1, m_2) &= \ell(\Psi^*(m_1, m_2)) \\ &= \ell(\sum_i \Psi(m_1, f_i m_2) e_i) \\ &= \sum_i \Psi(m_1, f_i m_2) \ell(e_i) \\ &= \Psi(m_1, \sum_i \ell(e_i) f_i m_2) \\ &= \Psi(m_1, m_2),\end{aligned}$$

since in R we can write $1 = \sum L(1, e_i) f_i = \sum \ell(e_i^*) f_i = \sum \ell(e_i) f_i$. The proposition follows.◇

Lemma 1.12. *Suppose that J acts non-trivially on k, and let Δ be the group $\{1, *\}$. Then the Δ-modules R^+ and $R^\times$ are cohomologically trivial.*

PROOF The additive group R^+ has a filtration given by the powers of the maximal ideal $\mathcal{M}$ which is stable under the action of the involution, giving for $0 \le i \le q-1$ the exact sequences of Δ-modules,

$$0 \longrightarrow \mathcal{M}^{i+1} \longrightarrow \mathcal{M}^i \xrightarrow{\epsilon} k \longrightarrow 0, \tag{1.19}$$

where $\epsilon(x) = x \bmod \mathcal{M}^{i+1}$. Now $\hat{H}^j(\Delta, k) = 0$: for $j = 0$ because the trace map is surjective from k onto the fixed field of J; and for $j = 1$ by the additive version of Hilbert's Theorem 90. From the long exact cohomology sequence associated to (1.19), we find that $\hat{H}^j(\Delta, \mathcal{M}^i) \cong \hat{H}^j(\Delta, \mathcal{M}^{i+1})$ for $0 \le i \le q-1$, and hence

$$\hat{H}^j(\Delta, R^+) = \hat{H}^j(\Delta, \mathcal{M}^0) \cong \hat{H}^j(\Delta, \mathcal{M}) \cong \ldots \cong \hat{H}^j(\Delta, \mathcal{M}^{q-1}) \cong 0.$$

In a similar way, we filter the multiplicative group $R^\times$ by the subgroups of "principal units" $U_i = 1 + \mathcal{M}^i$ for $1 \le i \le q-1$, $U_q = 1$. This filtration gives the following exact sequences of Δ-modules:

$$1 \longrightarrow U_1 \longrightarrow R^\times \xrightarrow{\epsilon_0} k^\times \longrightarrow 1, \qquad (1.20),$$

$$1\longrightarrow U_{i+1}\longrightarrow U_i \xrightarrow{\epsilon_i} k^+ \longrightarrow 0, \tag{1.21}$$

where ϵ_0 is the augmentation map and where $\epsilon_i(x) = x - 1 \bmod \mathcal{M}^{i+1}$. Now $\hat{H}^j(\Delta, k^+) = 0$: for $j = 0$ because the norm map is surjective from k to the fixed field of J (see Bourbaki, [Bo 2]); and for $j = 1$ by the multiplicative version of Hilbert's Theorem 90. From the long exact sequence associated to (1.20), we deduce that $\hat{H}^j(\Delta, R^\times) \cong \hat{H}^j(\Delta, U_1)$, and for $1 \le i \le q-1$ the long exact sequence associated to (1.21) gives $\hat{H}^j(\Delta, U_i) \cong \hat{H}^j(\Delta, U_{i+1})$. It follows that $R^\times$ is cohomologically trivial, since $U_q = 1$ has trivial cohomology.◇

Proposition 1.8. *Assuming still that J acts nontrivially on k, there is, up to equivalence, one class of nondegenerate Hermitian forms on the free R-module M of given rank n. More precisely, every Hermitian form Φ has an orthonormal basis.*

PROOF The proof is by induction on the rank n of M. Let first $n = 1$, and let χ be a generator of the free R-module M; since for any $\lambda_1, \lambda_2 \in R$,

$$\Phi(\lambda_1\chi, \lambda_2\chi) = \lambda_1\lambda_2^*\Phi(\chi, \chi),$$

the form Φ is determined by the element $d_\Phi = \Phi(\chi, \chi)$. Since Φ is Hermitian, d_Φ is fixed by $*$, and conversely, any such d determines a Hermitian form. Φ' is an equivalent form if there is a unit $u \in R$ such that $\Phi(u\chi, u\chi) = \Phi'(\chi, \chi)$, so that $uu^*d_\Phi = d_{\Phi'}$. It follows that the equivalence classes of Hermitian forms on M are in one-to one correspondence with the elements of the cohomology group $\hat{H}^0(\Delta, R^\times)$, which is trivial by lemma 1.12. In particular, we may find a generator χ such that $\Phi(\chi, \chi) = 1$.

Let now Φ be a nondegenerate Hermitian form on the free R-module M of rank $n+1$, and let χ_1 be a generator. If $\Phi(\chi_1, \chi_1) = u$ is a unit, then (Φ being Hermitian) u is fixed by the involution; by the lemma there is a unit v such that $vuv^* = 1$, so $\chi' = v\chi_1$ generates a free submodule of M, and

$$\Phi(\chi', \chi') = 1. \tag{1.22}$$

If u is not a unit, we can (by the nondegeneracy of Φ) find a χ_2 with $\Phi(\chi_1, \chi_2) = 1$. If $\Phi(\chi_2, \chi_2)$ is a unit, proceed as above to find a χ' such that $\Phi(\chi', \chi') = 1$. If both $\Phi(\chi_1, \chi_1)$ and $\Phi(\chi_2, \chi_2)$ are in the maximal ideal M, choose λ such that $\lambda + \lambda^* = 1$—this can be done by lemma 1.12—and let $\chi = \chi_1 + \lambda\chi_2$. Then χ is a generator of a free submodule of M, and

$$\Phi(\chi, \chi) = \Phi(\chi_1, \chi_1) + \lambda\lambda^*\Phi(\chi_2, \chi_2) + (\lambda + \lambda^*)\Phi(\chi_1, \chi_2)$$

is a unit in R. Again by the procedure above, we can find a χ' which generates a free submodule of M, such that (1.22) is satisfied.

Let $M_0 = R\chi'$, with χ' satesfiing (1.22). Then the restriction of Φ to M_0 is nondegenerate; as usual, let

$$M_0^\perp = \{m \in M, \Phi(m, m_1) = 0 \text{ for all } m_1 \in M_0.$$

$M_0^\perp$ is clearly an R-module, and by using the same idea as in the proof of lemma 1.1, it follows that $M = M_0 \oplus M_0^\perp$. By the Krull-Schmidt theorem, M_0 is free of rank n, and (as in lemma 1.1) the restiction of Φ to $M_0^\perp$ is nondegenerate. By induction $M_0^\perp$ has an orthonormal basis, hence so does M.◇

Corollary. *Let $R = k[G_2]$ with involution given by (1.17), and suppose that J acts non-trivially. If M is a free R-module of rank n, then all R-invariant forms $\Phi: M \times M \to \mathbb{F}_2$ are isometric.*

PROOF This follows from propositions 1.7 and 1.8.◇

Proposition 1.9. *Let G be a finite Abelian group with cyclic 2-Sylow subgroup G_2, let H be the subgroup of G of elements of order prime to 2, and let $\Lambda = \mathbb{F}_2[G]$. If M is a free Λ-module of rank n, then the isometry class of the symplectic space $\{M, \Phi, G\}$ is uniquely determined by the class of the symplectic space $\{E_1 M, \Phi, G_2\}$, where E_1 is the primitive idempotent $Sp_H \in \Lambda$.*

PROOF Let E_i be the idempotents defined in § 1.5, and let $\Lambda E_i = R_i$. From lemma 1.11 it follows that the isometry classes the symplectic space $\{M, \Phi, G\}$ is uniquely determined by the isometry classes of the symplectic spaces $\{E_i M, \Phi, R_i\}$. For $2 \leq i \leq r_1$ the corollary to proposition 1.8 implies that for a given rank n of the free Λ-module M, there is a unique class of symmetric, nondegenerate, R_i-invariant form on $E_i M$. For $r_1 + 1 \leq i \leq r_1 + r_2$, the restiction of any nondegerate form Φ to $E_i M$ possesses a hyperbolic decomposition: $e_i M \oplus e_i^* M$, and hence by lemma 1.2, the isometry class of $\{E_i M, \Phi, R_i\}$ is again uniquely determined by the rank n. Hence, the isometry class of the form Φ on M is determined by the isometry class of $\{E_1M, \Phi, R_1\}$. The inclusion $G_2 \hookrightarrow G$ induces an isomorphism of $\mathbb{F}_2$-algebras $\mathbb{F}_2[G_2] \cong \Lambda E_1 = R_1$ which is compatible with the respective actions of G_2 and R_1 on E_1M; hence, the spaces $\{E_1M, \Phi, G_2\}$ and $\{E_1M, \Phi, R_1\}$ are isometric.◇

Remark. Let $\overline{G} = G/H$, and let $\overline{\Lambda} = \mathbb{F}_2[\overline{G}]$. Since $\ker(\Lambda \xrightarrow{E_1} \Lambda) = \ker(\Lambda \longrightarrow \overline{\Lambda})$, we may identify R_1 with $\overline{\Lambda}$, and this identification is compatible with the natural action of $\overline{G}$ on E_1M. Thus the symplectic space $\{M, \Phi, G\}$ uniquely defines the symplectic space $\{\overline{M}, \overline{\Phi}, \overline{G}\}$, where we are writing $\overline{M} = M/\ker(M \xrightarrow{E_1} M)$ and $\overline{\Phi}$ for the induced form.

One can extend the definition of "form with trace condition" to G-invariant forms Φ in the obvious way: if S is a subgroup of G, then for all $x \in M$, $\Phi(x, x) = \Phi(x, Sp_S.x)$.

Lemma 1.13. *The symplectic space $\{M, \Phi, G\}$ has the trace condition if and only if the space $\{M, \Phi, G_2\}$ has the trace condition.*

PROOF The condition is certainly necessary. On the other hand, if S is an arbitrary subgroup of G, write $S = TU$ with T the 2-Sylow subgroup of S and U the subgroup of elements of S of order prime to 2. Assume that $\{M, \Phi, G_2\}$ has the trace condition. Then,

$$\begin{aligned}\Phi(x, Sp_S.x) &= \Phi(x, Sp_T Sp_U.x)\\ &= \Phi(Sp_U.x, Sp_T Sp_U.x)\\ &= \Phi(Sp_U.x, Sp_U.x)\\ &= \Phi(x, Sp_U.x).\end{aligned}$$

Because U has odd order, the only element of U fixed by the involution $.*$ is the identity element—all other elements are interchanged in pairs. The anti-symmetry of Φ shows that for $\tau \in U$, $\tau \neq 1$, $\Phi(x, (\tau + \tau^{-1}).x) = 0$, from which it follows that $\Phi(x, Sp_U.x) = \Phi(x, x)$.◇

Proposition 1.10. *We retain the hypotheses of proposition 1.9. Let Φ be a symplectic trace-form on the free Λ-module of rank n. Then Φ belongs to one of two isometry classes, distinguished by the Koch invariant of the space $\{Sp_H M, \Phi, G_2\}$ (or equivalently, by the Koch invariant of $\{\overline{M}, \overline{\Phi}, \overline{G}\}$).*

PROOF This all follows immedeately from proposition 1.9 and lemmas 1.10 and 1.13.◇

Let σ be a generator of G_2, and let $\pi = \sigma - 1$. By proposition 1.10, the structure of the space $\{M, \Phi, G\}$ is determined by the invariant ι of the space $\{Sp_H.M, \Phi, G_2\}$. Let θ_0 represent the homomorphism $\chi \mapsto \Phi(\chi, \chi)$ in $Sp_H.M$, and let $\theta \in Sp_H.M$ be such that $Sp_{G_2}\theta = \theta_0$. Then $\iota = \Phi(\theta, \pi^{q-2}\theta)$. If $\xi \in M$ is such that $Sp_G\xi = \theta_0$, then

$$\begin{aligned}\Phi(\xi, \pi^{q-2} Sp_H \xi) &= \Phi(Sp_H \xi, \pi^{q-2} Sp_H \xi)\\ &= \iota.\end{aligned}$$

We will call ι the invariant of the space $\{M, \Phi, G\}$.

Proposition 1.11. *Let n be the rank of the symplectic space $\{M, \Phi, G\}$, and let $\iota = \iota_M$ be the invariant. The isometry class of this space is completely determoned by these invariants. In particular, there exist Λ-free generators $\chi_1, \ldots, \chi_n$ such that Φ takes the following values: (i) If n is odd,*

$$M = \Lambda\chi_1 \perp \langle \Lambda\chi_2 + \Lambda\chi_3 \rangle \perp \ldots \perp \langle \Lambda\chi_{n-1} + \Lambda\chi_n \rangle,$$

with $\Lambda\chi_i$ totally isotropic for $2 \le i \le n$, and for $i \ge 1$,

$$\Phi(\chi_{2i}, g\chi_{2i+1}) = \begin{cases} 1, & \text{if } g \ne 1;\\ 0, & \text{otherwise,}\end{cases}$$

and

$$\Phi(\chi_1, g\chi_1) = \begin{cases} 1, & \text{if } g = 1;\\ \iota + 1, & \text{if } g = \sigma, \sigma^{-1};\\ 0, & \text{otherwise;}\end{cases}$$

the values of Φ on other generators being determined by the G-invariance and the symmetry. (ii) If n is even,

$$M = \Lambda\chi_1 \perp \Lambda\chi_2 \perp \langle \Lambda\chi_3 + \Lambda\chi_4 \rangle \perp \ldots \perp \langle \Lambda\chi_{n-1} + \Lambda\chi_n \rangle.$$

Here, the $\Lambda\chi_i$ are totally isotropic for $3 \le i \le n$; for $2 \le i \le n/2$,

$$\Phi(\chi_{2i-1}, g\chi_{2i}) = \begin{cases} 1, & \text{if } g = 1;\\ 0, & \text{otherwise;}\end{cases}$$

$$\Phi(\chi_1, g\chi_1) = \begin{cases} 1; & \text{if } g = 1;\\ \iota + 1, & \text{if } g = \sigma, \sigma^{-1};\\ 0, & \text{otherwise;}\end{cases}$$

$$\Phi(\chi_2, g\chi_2) = \begin{cases} 1, & \text{if } g = 1;\\ 0, & \text{otherwise.}\end{cases}$$

All other values of Φ on generators of M are determined from these ones by G-invariance and symmetry.

PROOF That the invariants n and ι_M determine the isometry class of M follows from proposition 1.9; the particular representatives given in (i) and (ii) are easily shown to have the proper invariant.◇

Chapter 2. The Symplectic Structure of the Hilbert Symbol.

§2.1 We begin this chapter with an example of G-invariant forms coming from finite fields. Let k be a finite extension of $\mathbf{F}_2$ of degree f_0, and let K/k be a finite extension of k of order f and Galois group G—we will assume throughout this section that 4 divides f. As is well known (see, *e.g.*, [La 1]), the group G is cyclic of order f, generated by the "Frobenius automorphism" σ: $\sigma.x = x^{2^{f_0}}$ for all $x \in K$. Furthermore, the extension K/k possesses a normal basis: there is a $\xi \in K$ such that

$$K = \bigoplus_{g \in G} kg.\xi;$$

in other words, K is free of rank one as a $k[G]$-module. Since k itself is of rank f_0 over $\mathbf{F}_2$, it follows that as an $\mathbf{F}_2[G]$-module, K is free of rank f_0.

Define the $\mathbf{F}_2$-bilinear form $\Phi = \Phi_{K/k} : K \times K \to \mathbf{F}_2$ by

$$\Phi(x,y) = \mathrm{tr}_{K/\mathbf{F}_2}(xy).$$

Φ is certainly symmetric, and is nondegenerate since the trace map is surjective for extensions of finite fields ([Bo 1],chapter V,§ 11). Letting $G' = \mathrm{Gal}(K/\mathbf{F}_2)$, we have for any $g \in G$,

$$\begin{aligned}\Phi(g.x, g.y) = \mathrm{tr}_{K/\mathbf{F}_2}(g.(xy)) &= \sum_{g' \in G'} g'.(g.(xy)) \\ &= \sum_{g' \in G'} (g'g).(xy) \\ &= \Phi(x,y),\end{aligned}$$

so that Φ is G-invariant. Finally, Φ is a non-alternating trace-form: indeed, for $x \in K$,

$$\Phi(x,x) = \mathrm{tr}_{K/\mathbf{F}_2}(x^2) = (\mathrm{tr}_{K/\mathbf{F}_2}(x))^2 = \mathrm{tr}_{K/\mathbf{F}_2}(x),$$

and this is non-zero for some x by surjectivity of the trace. Note that this computation also shows that $\Phi(x,x) = \Phi(x,1)$. If $\rho^2 = 1$ in G, and if K' is the fixed field of $\{1,\rho\}$, then

$$\Phi(x,\rho.x) = \mathrm{tr}_{K'/\mathbf{F}_2} \circ \mathrm{tr}_{K/K'}(x\rho.x) = \mathrm{tr}_{K'/\mathbf{F}_2}(2x\rho.x) = 0,$$

since $x\rho.x \in K'$. It follows from lemma 1.13 and the discussion prior to proposition 1.3 that Φ is a trace-form. Let $\iota_{K/k}$ be the invariant of the space $\{K, \Phi_{K/k}, G\}$.

Lemma 2.1. *Let H be the subgroup of G of elements of order prime to 2, let $\overline{G} = G/H$, and let K_0 be the fixed-field of H. Then $\iota_{K/k} = \iota_{K_0/k}$.*

PROOF If ξ is a generator of a normal basis of K/k, then $\mathrm{tr}_{K/k}\xi = \eta \neq 0$, and by letting $\xi' = \xi\eta^{-1}$, we may assume that $\mathrm{tr}_{K/k}\xi = 1$. By the discussion following proposition 1.10,

$$\begin{aligned}\iota_{K/k} &= \Phi(\xi, \pi^{q-3} Sp_H \xi) \\ &= \Phi(Sp_H\xi, \pi^{q-3} Sp_H \xi) \\ &= \mathrm{tr}_{K/\mathbb{F}_2}((Sp_H\xi)(pi^{q-3} Sp_H\xi)) \\ &= \mathrm{tr}_{K_0/f_2}(Sp_H(Sp_H\xi(\pi^{q-3} Sp_H\xi)) \\ &= \mathrm{tr}_{K_0/\mathbb{F}_2}(Sp_H\xi(\pi^{q-3} Sp_H\xi)),\end{aligned}$$

since H has odd order. Now $Sp_H\xi = \overline{\xi}$ has $\mathrm{tr}_{K_0/k}(\overline{\xi}) = 1$, so that

$$\begin{aligned}\mathrm{tr}_{K_0/k}(\overline{\xi}, \pi^{q-3}\overline{\xi}) &= \Phi_{K_0/k}(\overline{\xi}, \pi^{q-3}\overline{\xi}) \\ &= \iota_{K_0/k}. \quad \diamond\end{aligned}$$

Now suppose that $[K:k] = q$ is a power of 2, let L be the maximal subfield of K which is of 2-power degree over $\mathbb{F}_2$, and let $W = \mathrm{Gal}(K/L)$. Let $l = k \cap L$; l is the subfield of $K/\mathbb{F}_2$ fixed by the group generated by W and G.

Lemma 2.2. $\iota_{K/k} = \iota_{L/l}$.

PROOF Let $\xi \in K$ be such that $Sp_G.\xi = \mathrm{tr}_{K/k}\xi = 1$. Then $Sp_G(Sp_W.\xi) = Sp_W Sp_G.\xi = Sp_W.1 = 1$, so that we may assume ξ was choosen in L. Then

$$\begin{aligned}\iota_{K/k} = \mathrm{tr}_{K/\mathbb{F}_2}((\xi)(\pi^{q-3}.\xi)) &= \mathrm{tr}_{L/\mathbb{F}_2} \circ \mathrm{tr}_{K/L}((\xi)(\pi^{q-3}.\xi)) \\ &= \mathrm{tr}_{L/\mathbb{F}_2}((\xi)(\pi^{q-3}.\xi)) \\ &= \Phi_{L/l}(\xi, \pi^{q-3}.\xi) \\ &= \iota_{L/l}. \diamond\end{aligned}$$

Lemma 2.3. *Suppose that K/k is of 2-power degree q, and that $k/\mathbb{F}_2$ is of 2-power degree f_0. Let K' be the subfield of degree 4 over k. Then $\iota_{K/k} = \iota_{K'/k}$.*

PROOF Let $\mathrm{tr}_{K/k}(\xi) = 1$, so that

$$\iota_{K/k} = \mathrm{tr}_{K/\mathbb{F}_2}((\xi)(\pi^{q-3}.\xi)) = \mathrm{tr}_{K'/\mathbb{F}_2} \circ \mathrm{tr}_{K/K'}((\xi)(\pi\pi^{4(q/4-1)}.\xi)).$$

But σ^4 generates the subgroup $H = \mathrm{Gal}(K/K')$, and $\pi^{4(q/4-1)} = (1+\sigma^4)^{q/4-1} = Sp_H$. With $\theta = Sp_H\xi = \mathrm{tr}_{K/K'}(\xi)$, we have

$$\begin{aligned}\iota_{K/k} &= \mathrm{tr}_{K'/\mathbf{F}_2}(\mathrm{tr}_{K/K'}(\xi(\pi.\theta)) = \mathrm{tr}_{K'/\mathbf{F}_2}((\mathrm{tr}_{K/K'}(\xi))(\pi.\theta)) \\ &= \mathrm{tr}_{K'/\mathbf{F}_2}(\theta(\pi.\theta)) \\ &= \iota_{K'/k}.\diamond\end{aligned}$$

Lemma 2.4. *For $K/\mathbf{F}_2$ of 2-power order, $\iota_{K/\mathbf{F}_2} = 0$.*

PROOF By lemma 2.3, it suffices to compute ι for $K/\mathbf{F}_2$ of order 4. In this case, a normal basis of $K/\mathbf{F}_2$ is generated by a primitive fifth root of unity ξ (since $\mathrm{tr}_{K/\mathbf{F}_2} = 1$), and the galois group G is generated by the Frobenius $\sigma: x \mapsto x^2$ for all $x \in K$. Then

$$\begin{aligned}\iota_{K/\mathbf{F}_2} &= \mathrm{tr}_{K/\mathbf{F}_2}(\xi(\pi.\xi)) = \mathrm{tr}_{K/\mathbf{F}_2}(\xi(\xi+\xi^2)) \\ &= \mathrm{tr}_{K/\mathbf{F}_2}(\xi^2+\xi^3) \\ &= 0,\end{aligned}$$

since both ξ^2 and ξ^3 are conjugates of ξ, and hence each has trace 1.◇

Proposition 2.1. *Let k be a finite extension of $\mathbf{F}_2$ of degree f_0, and let K/k be a finite extension of order q divisible by 4, with Galois group G generated by the Frobenius automorphism σ. Then the invariant $\iota_{K/k}$ is given by the parity of $f_0 + 1$.*

PROOF By lemmas 2.1, 2.2, and 2.4, we may assume that $k/\mathbf{F}_2$ is of 2-power order f_0, and $q = 4$. Let $\tilde{G} = \mathrm{Gal}(K/\mathbf{F}_2)$, and let s be the Frobenius automorphism $x \mapsto x^2$, so that $s^{f_0} = \sigma$. Let ξ generate a normal basis for $K/\mathbf{F}_2$; by lemma 2.4 and the proof of lemma 1.9, ξ can be chosen so that,

$$\mathrm{tr}_{K/\mathbf{F}_2}(\xi\xi^{s^i}) = \begin{cases} 1, & \text{if } i = -1,0,1; \\ 0, & \text{otherwise.}\end{cases} \tag{2.1}$$

Letting $\theta = \sum_{i=0}^{f_0-1} \xi^{s^i}$, it follows that $\mathrm{tr}_{K/k}(\theta) = 1$. If $k = \mathbf{F}_2$ we are done by lemma 2.4, while for $k/\mathbf{F}_2$

a non-trivial extension, we have $\mathrm{tr}_{K/\mathbb{F}_2}(\theta^2) = 0$, so

$$\begin{aligned}\iota_{K/k} &= \mathrm{tr}_{K/\mathbb{F}_2}((\theta)\cdot(1+\sigma)\theta)\\ &= \mathrm{tr}_{K/\mathbb{F}_2}(\theta^2) + \mathrm{tr}_{K/\mathbb{F}_2}(\theta\cdot\sigma\theta)\\ &= \mathrm{tr}_{K/\mathbb{F}_2}(\sum_{i=0}^{f_0-1}\xi^{s^i}\cdot s^{f_0}\sum_{j=o}^{f_0-1}\xi^{s^j})\\ &= \sum_{i,j}\mathrm{tr}_{K/\mathbb{F}_2}(\xi^{s^i}\xi^{s^{f_0+j}})\\ &= \sum_{i,j}\mathrm{tr}_{K/\mathbb{F}_2}(\xi\cdot\xi^{s^{f_0+j-i}}).\end{aligned}$$

Now $f_0+j-i \equiv 1 \pmod{4f_0}$ only if $j=0$ and $i = f_0-1$, and cannot take on the values 0 or -1. From (2.1) it follows that $\iota_{K/k} = 1$.◇

§ 2.2 The second application of our structure theorem concerns the symplectic structure of the Hilbert symbol in unramified (and hence, Abelian) extensions of 2-adic number fields. Our main result (proposition 2.4) is an extension of Satz 9 of Koch [Ko 3]. We begin by reviewing the definition of the Hilbert symbol for local fields—for the details, see [Sh 1], [S 1], or [Ko 2].

For the time being, let p be any prime, and let K be a so-called "irregular" p-adic number field—that is, K contains the p^s roots of unity μ_{p^s} for some $s \geq 1$. Let Ω be a fixed algebraic closure of K, and let $X_K = \mathrm{Gal}(\Omega/K)$ be the absolute Galois group of K. Kummer theory gives a group homomorphism

$$\kappa: K^\times \to \mathrm{Hom}(\mathrm{X_K}, \mu_{p^s}), \tag{2.1}$$

defined as follows: given any element $a \in K^\times$, let $\alpha = a^{1/p^s}$ be any solution in Ω of $x^{p^s} - a = 0$. Given $\sigma \in X_K$, let

$$\kappa(a)(\sigma) = \frac{\sigma\alpha}{\alpha} \in \mu_{p^s}.$$

κ is surjective, and its kernel is precisely the subgroup of p^s-powers in $K^\times$, thus inducing an isomorphism (which we will also call κ)

$$A_K = \frac{K^\times}{K^{\times p^s}} \cong \mathrm{Hom}(\mathrm{X_K}, \mu_{p^s}).$$

On the other hand, the reciprocity map of local class field theory gives an injective group homomorphism

$$\theta_K : K^\times \to X_K^{\mathrm{ab}}.$$

One can thus define the pairing,

$$(\ ,\ )_K : K^\times \times K^\times \to \mu_{p^s},$$

$$(a, b)_K = \kappa(a)(\theta_K(b)).$$

This is the (p^s-) Hilbert symbol for the field K, and gives a bi-multiplicative form whose left- and right- kernels contain the subgroup $K^{\times p^s}$, thus inducing a form (also denoted by $(\ ,\ )_K$) on the free $\mathbb{Z}/p^s\mathbb{Z}$-module $A_K = K^\times/K^{\times p^s}$.

Remark. Throughout this section, we will retain the multiplicative notation, but if ς is a generator of μ_{p^e}, we may (non-canonically) identify μ_{p^e} with $\mathbb{Z}/p^e\mathbb{Z}$ (as Abelian groups) by means of the map

$$a \bmod p^e \leftrightarrow \varsigma^a.$$

If the group G acts on μ_{p^e}, we may define a (canonical!) homomorphism $\alpha\colon G \longrightarrow \mathbb{Z}/p^e\mathbb{Z}^\times$ so that

$$\varsigma^g = \varsigma^{\alpha(g)}.$$

Define now the "twisted" action of G on $\mathbb{Z}/p^e\mathbb{Z}$ by $g.1 = \alpha(g)$, and let $\mathbb{Z}/p^e\mathbb{Z}(\alpha)$ denote the resulting G-module. Then $\mu_{p^e} \cong \mathbb{Z}/p^e\mathbb{Z}(\alpha)$ as G-modules. With this identification, we may consider the Hilbert symbol to be an anti-symmetric, G-invariant bilinear form in the sense of chapter 1.†

Proposition 2.2. *The Hilbert symbol $(\ ,\ )_K$ has the following properties:*

(i) $(\ ,\ )_K$ is a nondegenerate, anti-symmetric bilinear form on A_K;

(ii) $(a,a)_K = (a,-1)_K$ for all $a \in K^\times$;

(iii) $(a, 1-a)_K = 1$ for all $a \neq 0,1$;

(iv) If K is a finite extension of L, and L also contains the p^e roots of unity, then

$$(a,b)_K = (a, N_{K/L}b)_L$$

for all $a \in L^\times$ and $b \in K^\times$ ($N_{K/L}$ is the usual field-theoretic norm from K to L);

(v) $(a,b)_K = 1$ for all $b \in K^\times$ if and only if a is a p^e-power in K.

(vi) $(a,b)_K = 1$ if and only if a is a norm from $K(b^{\frac{1}{p^e}})$ (for which reason $(\ ,\ )_K$ is sometimes called the "norm-residue" symbol);

(vii) If K/k is Galois with group G, then the pairing is G-invariant:

$$(\sigma a, \sigma b)_K = (a,b)_K^\sigma$$

for all $\sigma \in G$.

† The involution on the group ring $\mathbb{Z}/p^e\mathbb{Z}G$ being $(\sum a_g g)^* = \sum a_g \alpha(g) g^{-1}$. In the sequel the α will be trivial.

PROOF This is all well-known. See, for example, [Ko 1], § 8.11. ◇

Remark. Property (iv) can be interpretted in terms of the commutative diagram,

$$\begin{tikzcd}
A_K \times A_K \arrow[r, "(\, , \,)_K"] \arrow[d, shift right=8, "N_{K/L}"'] & \mu_{p^e} \arrow[d, equal] \\
A_L \times A_L \arrow[r, "(\, , \,)_L"] \arrow[u, shift left=8, "i_{K/L}"'] & \mu_{p^e}
\end{tikzcd} \tag{2.2}$$

Here, the first vertical arrow is the map induced by the norm, while the second vertical arrow is the map induced by the inclusion $L \rightarrow K$.

Lemma 2.5. *Suppose that K/k is Galois with group G, and suppose that k contains the p^e roots of unity. Then $(\, , \,)_K$ is a trace-form.*

PROOF Let H be a subgroup of G, and let L be the fixed-field of H. First note that if $a \in K^\times$ and if $\bar{a}$ denotes the image of a in A_K, then $Sp_H \bar{a} = i_{K/L}(\overline{N_{K/L}a})$. Thus for any $a \in K^\times$,

$$\begin{aligned}
(a,a)_K &= (a,-1)_K \\
&= (N_{K/L}a,-1)_L \\
&= (N_{K/L}a, N_{K/L}a)_L \\
&= (a, N_{K/L}a)_K. \quad \diamond
\end{aligned}$$

Let k be a p-adic number field containing the p^e-roots of unity, and let θ be a uniformising parameter for k. A p^e-primary number in k is a β such that $k(\beta^{\frac{1}{p^e}})$ is the unique unramified extension of k of degree p^e. Because of the nondegeneracy of the Hilbert symbol and the fact that every unit of k is a norm from any unramified extension of k (see, *e.g.*, [Sh 1] proposition 58), it follows that $(\theta,\beta)_k$ is a primitive p^e root of unity. Again, because β is a norm from $k(\beta^{\frac{1}{p^e}})$, $(\beta,\beta)_k = 1$. If $p \neq 2$, then the anti-symmetry of the Hilbert symbol implies $(\theta,\theta)_k = 1$.

Lemma 2.6. *Suppose that the 2-adic number field k doesn't contain the fourth roots of unity, and suppose that $k(\sqrt{-1})$ is ramified over k. Then a uniformising parameter θ can be found so that $(\theta,\theta)_k = 1$.*

PROOF The extension $k((-1)^{1/2})/k$ is unramified if and only if $1 = (u,-1)_k = (u,u)_k$ for all units $u \in k^\times$. Thus, if $k((-1)^{1/2})/k$ is ramified, there is a unit $u \in k$ so that $(u,u)_k = -1$. If θ is any uniformising parameter, and $(\theta,\theta)_k = -1$, then the uniformising parameter $\theta' = u\theta$ will work.◇

Let k be a p-adic number field containing the p^e roots of unity (with p arbitrary), and let K be a tamely ramified extension of k having Galois group G. Let θ be a uniformizing parameter of k, and let β be a p^e-primary element of K.

Proposition 2.3. *The subgroup of A_K generated by the images of θ and β is free of rank 2 over $\mathbb{Z}/p^e\mathbb{Z}$ and is stable under the action of G. The Hilbert symbol is nondegenerate on this subspace, and the orthogonal complement $M_K = M_{K,\theta}$ is a free $\mathbb{Z}/p^e\mathbb{Z}[G]$-module of rank $n = [k : \mathbb{Q}_p]$, on which $(\ ,\ )_K$ restricts to a nondegenerate, anti-symmetric, G-invariant form.*

PROOF Proof of the proposition involves a detailed examination of explicit reciprocity formulae given by the "Shafarevich E-function" ([Sha 1]). For $p \neq 2$, this theorem is contained in [Ja 1], lemmas 23 and 24. For $p = 2$, see Sats 9 of [Ko 3] or theorem 2 of [Z 1].◇

§ 2.3 We now restrict our attention to the following situation: k is a 2-adic number field of degree $n = e_0 f_0$ over $\mathbb{Q}_2$, e_0 being the ramification index and f_0 the residue degree of the extension $k/\mathbb{Q}_2$. Let K be an unramified (Abelian) extension of k with Galois group G of order qq', where q is of 2-power order and q' is prime to 2. We further suppose that 4 divides q, and that K doesn't contain ~~the fourth~~ roots of unity.

As in the previous section, let θ be a uniformizing parameter for k, β a 2-primary element of K, and M_K the complement of the subspace generated by (the images of) θ and β in A_K.

Lemma 2.7. *The restriction of the Hilbert symbol to M_K is non-alternating.*

PROOF Since $K(\sqrt{\beta})/K$ is unramified, -1 is a norm from $K(\sqrt{\beta})$, so by (vi) of proposition 2.2, $(\beta, -1) = 1$; since K/k is even,

$$\begin{aligned}(\theta, -1)_K &= (N_{K/k}\theta, -1)_k \\ &= (\theta^{qq'}, -1)_k \\ &= 1,\end{aligned}$$

so that $\overline{-1} \in M_K$. Since -1 is not a square, the nondegeneracy of the symbol insures the existence of an $\bar{a} \in M_K$ with

$$-1 = (a, -1)_K = (a, a)_K. \quad \diamond$$

In view of proposition 2.3 and lemma 2.7, we denote by $\iota_{K/k}$ the Koch invariant of the symplectic space $\{M_K, (\ ,\ )_K, G\}$.

Lemma 2.8. *Let L be the maximal subfield of K of 2-power order over k, let $H = \mathrm{Gal}(K/L)$, and let $\overline{G} = G/H \cong \mathrm{Gal}(L/k)$. If β_0 is a 2-primary element of L, and M_L is the complement in A_L of the subspace generated by θ and β_0 with respect to the form $(\ ,\ )_L$, then the invariants $\iota_{K/k}$ of $\{M_K, (\ ,\ )_K, G\}$ and $\iota_{L/k}$ of $\{M_L, (\ ,\ )_L, \overline{G}\}$ are equal.*

PROOF First note that we may take β_0 as our 2-primary element of K, since K/L is of odd degree q'; the oddness of q' also implies that the maps $N_{K/L}$ and $i_{K/L}$ of diagram 2.2 are, repectively, surjective and injective. We claim that $i_{K/L}(M_L) = Sp_H.M_K$. Indeed, given $\overline{a} \in M_L$,

$$Sp_H.i_{K/L}(\overline{a}) = i_{K/L}(\overline{a})^{q'} = i_{K/L}(\overline{a}),$$

so that $i_{K/L}(M_L) \subseteq Sp_H.M_K$. On the other hand, given any $a \in K^\times$,

$$Sp_H.\overline{a} = i_{K/L}(\overline{N_{K/L}a}),$$

so that if $\overline{a} \in M_K$, then

$$1 = (\theta, a)_K = (\theta, N_{K/L}a)_L,$$

$$1 = (\beta_0, a)_K = (\beta_0, N_{K/L}a)_L.$$

It follows that $N_{K/L}M_K \subseteq M_L$, and hence that

$$Sp_H.M_K = i_{K/L} \circ N_{K/L}(M_K) \subseteq i_{K/L}(M_L).$$

The symplectic spaces $\{M_L, (\ ,\ )_L, \overline{G}\}$ and $\{Sp_H.M_K, (\ ,\ )_K, \overline{G}\}$ are thus isometric, so by proposition 1.10 and the discussion following that proposition, $\iota_{L/k} = \iota_{K/k}$. ◇

The following proposition, due to Koch ([K 3], Satz 9), shows how the invariant of the form is dependent on the arithmetic of the field k.

Proposition 2.8. *(H. Koch) Let k be a 2-adic number field of degree $n = e_0 f_0$ over $\mathbb{Q}_2$, where e_0 is the ramification index and f_0 the residue degree of the extension $k/\mathbb{Q}_2$. Let K be the unramified extension of k with degree $q \geq 4$ of 2-power order over k. Assume that the fourth roots of unity do not lie in K. Then the invariant $\iota_{M_K} = \iota_{K/k} = \iota_k$ is,*

$$\iota_k = e_0(f_0 + 1).$$

PROOF Let G =Gal(K/k), and let σ be the Frobenius automorphism of K/k, hence a generator of G. By the proof of lemma 2.7, $\overline{-1} \in M_K$ represents the homomorphism $\chi \mapsto (\chi, \chi)_K$, so to compute $\iota_{K/k}$, we must compute $(\epsilon, \pi^{q-3}\epsilon)_K$ for some $\epsilon \in K$ with $Sp_G.\bar{\epsilon} = -1$ (recall that $\bar{\pi} = \sigma - 1$). Let T be the largest subfield of K which is unramified and of 2-power degree f over $\mathbb{Q}_2$, and let $T' = T \cap k$. Then $f = qf'$, f' being the degree of the extension $T'/\mathbb{Q}_2$. Let τ be the Frobenius of the extension $T/\mathbb{Q}_2$. Then the restriction of σ to T is $\tau^{f'}$. Let $\gamma \in T$ be such that $N_{T/\mathbb{Q}_2}\gamma = -1$, and let

$$\epsilon = \prod_{i=0}^{f'-1} \tau^i \cdot \gamma.$$

Then

$$N_{K/k}\epsilon = N_{T/T'}\epsilon = N_{T/\mathbb{Q}_2}\gamma = -1.$$

Now $\epsilon \in M_K$. Indeed, $(\beta, \epsilon)_K = 1$ since ϵ is a unit, and $(\theta, \epsilon)_K = (\theta, -1)_k = 1$ for θ chosen as in lemma 2.6. Thus

$$(\epsilon, \pi^{q-3}\epsilon)_K = (\epsilon^{[K:T]}, \pi^{q-3}\epsilon)_T = (\epsilon, \pi^{q-3}\epsilon)_T^{e_0}, \tag{2.3}$$

since $\frac{f}{f'}$ is odd.

We now compute $(\epsilon, \pi^{q-3}\epsilon)_T$ as in the proof of proposition 2.1. Namely, we may first assume that T/T' is of degree 4: if T_0 is the subfield of T of degree 4 over T', then $\pi^{q-4}\epsilon = N_{T/T_0}\epsilon$, and

$$\begin{aligned}(\epsilon, \pi^{q-3}\epsilon)_T &= (\epsilon, N_{T/T_0}(\pi\epsilon))_T \\ &= (N_{T/T_0}(\epsilon), \pi . N_{T/T_0}(\epsilon))_{T_0}.\end{aligned}$$

Suppose now that T has degree 4 over $T' = \mathbb{Q}_2$, and let ζ be a primitive fifth root of unity in T. Define $\epsilon_0 = 1 - 2\zeta$. Then $\overline{N_{T/\mathbb{Q}_2}\epsilon_0} = \overline{31} = \overline{-1}$ in $A_{\mathbb{Q}_2}$, and hence

$$\iota_{T/\mathbb{Q}_2} = (\epsilon_0, \pi\epsilon_0)_T.$$

Now

$$(\epsilon_0,\epsilon_0)_T = (\epsilon_0,-1)_T = (-1,-1)_{\mathbb{Q}_2} = -1.$$

To evaluate $(\epsilon_0,\sigma\epsilon_0)_T = (1-2\varsigma, 1-2\varsigma^2)_T$, we make use of the following formula, due to Kneser ([Kn 1], equation 13): for any $x,y \neq 0,1$ in T, let $a = \frac{y(1-x)}{1-xy}$. Then since $(a,1-a)_T = 1$, we have

$$\begin{aligned}
1 &= \left(\frac{y(1-x)}{1-xy}, \frac{1-y}{1-xy}\right)_T \\
&= (y, 1-xy)_T^{-1}(1-x,1-y)_T(1-x,1-xy)_T^{-1}(1-xy,1-y)_T^{-1}(1-xy,1-xy)_T \\
&= (-y,1-xy)_T^{-1}(1-x,1-y)_T(1-x,1-xy)_T^{-1}(1-xy,1-y)_T^{-1},
\end{aligned}$$

from which one obtains,

$$(1-x,1-y)_T = (-y,1-xy)_T(1-x,1-xy)_T(1-xy,1-y)_T. \tag{2.4}$$

With $x = 2\varsigma$ and $y = 2\varsigma^2$, equation (2.4) gives

$$(1-2\varsigma,1-2\varsigma^2)_T = (-2\varsigma^2,1-4\varsigma^3)_T(1-2\varsigma,1-4\varsigma^3)_T(1-4\varsigma^3,1-2\varsigma^2)_T.$$

If in equation (2.4) xy is an integer of T congruent to 0 (mod 8), then the principal unit $1-xy$ is a square in T (see, for example, [Shaf 1], page 79). It follows that

$$\begin{aligned}
(1-2\varsigma,1-2\varsigma^2)_T = (-2\varsigma^2,1-4\varsigma^3)_T &= (-2,1-4\varsigma^3)_T \\
&= (-2, N_{T/\mathbb{Q}_2}(1-4\varsigma^3))_{\mathbb{Q}_2} \\
&= (-2,5)_{\mathbb{Q}_2} \\
&= -1.
\end{aligned}$$

Thus $\iota_{T/\mathbb{Q}_2} = 0$.

Now assume that T/T' is unramified of 2-power degree q divisible by 4 (with Galois group generated by σ), and that $T'/\mathbb{Q}_2$ is unramified of 2-power degree $f' \neq 1$. One repeats the proof of proposition 2.1 *mutatis mutandis*, the only change being that the Hilbert symbol is being written multiplicatively. We conclude that in this case, $\iota_{T/T'} = \iota_{T'} = 1$.

It follows that in general, $\iota_{T'}$ is given by the parity of $f'+1$, and hence by the parity of f_0+1. We now obtain from (2.3) that ι_b is given by the parity of $e_0(f_0+1)$.◇

Corollary. *Let k be a 2-adic number field, and let K be an unramified extension of k having order divisible by 4, and not containing the fourth roots of unity. If e_0 and f_0 are, respectively, the ramification index and the residue degree of the extension $k/\mathbf{Q}_2$, the symplectic structure of the space $\{K^\times/K^{\times 2}, (\ ,\ )_K, \mathrm{Gal}(K/k)\}$ is determined by the invariant $\iota_{K/k} = \iota_k = e_0(f_0+1)$.*

PROOF From the proofs of lemmas 2.6 and 2.8, we may find a uniformizing parameter θ and a 2-primary unit β_0 so that

$$(\theta,\theta)_K = (\beta_0,\beta_0)_K = 1, \quad (\theta,\beta_0)_K = -1,$$

and,

$$K^\times/K^{\times 2} = \langle\theta,\beta_0\rangle \perp M_K.$$

As in proposition 1.11, we may choose generators of M_K with the values of the Hilbert symbol on these generators determined completely by the invariant $\iota_{K/k}$.◇

Chapter 3. Profinite Cohomology and Demuškin Groups

§ 3.1 This first section reviews some of the elementary aspects of profinite cohomology needed in the sequel. For more details, see [S 2], [Sh 1], or [Ko 2].

A profinite group X is a compact, totally disconnected topological group. A discrete X-module A is an Abelian group with the discrete topology on which X acts continuously. For U a closed subgroup of X, we denote by A^U the submodule of A fixed by U. Note that if U is a normal subgroup, then A^U is an X/U-module.

Let $C^n(X,A)$ be the group of continuous maps from X^n to A, and define the coboundary operators $\partial_n : C^n(X,A) \to C^{n+1}(X,A)$ by the usual formula,

$$(\partial_n f)(x_0,\ldots,x_n) = f(x_1,\ldots,x_n) + \sum_{i=1}^{n}(-1)^i f(x_0,\ldots,x_{i-1}x_i,\ldots,x_n) + (-1)^{n+1} f(x_0,\ldots,x_{n-1}).$$

We thus get the standard cochain complex $0 \to C^*(X,A)$ whose cohomology groups are $H^n(X,A) = \ker(\partial_n)/\operatorname{im}(\partial_{n-1})$, with $H^0(X,A)$ defined to be A^X.

Given an exact sequence of X-modules $0 \to A_1 \xrightarrow{\alpha} A_2 \xrightarrow{\beta} A_3 \to 0$, one obtains a "long exact sequence" of cohomology groups,

$$\ldots \longrightarrow H^{n-1}(X,A_3) \xrightarrow{\delta} H^n(X,A_1) \xrightarrow{\alpha^*} H^n(X,A_2) \xrightarrow{\beta^*} H^n(X,A_3) \xrightarrow{\delta} H^{n+1}(X,A_1) \longrightarrow \ldots,$$

where the maps α^* and β^* are induced from the maps on the cochains, and the connecting homomorphisms δ come from the "snake lemma" (see [Sh 1], page 19).

Let X and Y be profinite groups, and let A and B be, respectively, a discrete X-module and a discrete Y-module. One says that the pair of maps $\phi : X \to Y$ and $\psi : B \to A$ are compatible, if for any $x \in X$ and $b \in B$, $\psi(\phi(x).b) = x.\psi(b)$. One easily checks that any such compatible pair induces a map on the cohomology groups $(\phi,\psi)^* : H^q(Y,B) \to H^q(X,A)$, given on cocycles by

$$(\phi,\psi)^*(f)(x_1,\ldots,x_n) = \psi(f(\phi(x_1),\ldots,\phi(x_n))).$$

For example, if U is a normal subgroup of X with quotient G, and A is an X-module, then A^U is a G-module, and the maps $X \to G$ and $A^U \to A$ are compatible; the induced maps obtained on cohomology are the "inflation" homomorphisms, inf: $H^q(G, A^U) \to H^q(X, A)$. As another important example of this principle: with U still normal in X, define for $x \in X$ the maps $\phi_x : U \to U$ to be conjugation by x (where we use the convention $y \mapsto X^{-1}yx$), and $\psi_x : A \to A$ by $a \mapsto x.a$. The compatibility of the pair (ϕ_x, ψ_x) thus induces an action of X on the cohomology groups $H^n(U, A)$ in which U acts trivially. We thus have a natural action of $G \cong X/U$ on $H^n(U, A)$.

Let X be a profinite group, U a (closed) subgroup of X, and let A be a discrete U-module. Define the induced module,

$$M_X^U(A) = \{f : X \to A \quad \text{such that} \quad f(ux) = u.f(x) \quad \text{for all} \quad u \in U \quad \text{and} \quad x \in X\}.$$

The induced module carries an X-action defined by $(x.f)(y) = f(yx)$ for all $x, y \in X$. This action is compatible with the X-module homomorphism $M_X^U(A) \to A$ defined by $f \mapsto f(1)$, and we thus get a map on the cohomology groups $H^q(X, M_X^U(A)) \to H^q(U, A)$, which is an isomorphism by Shapiro's lemma [Ko 2]. Using this, we can define the standard "change of group" maps on cohomology : if A is an X-module, define the X-module homorphism $i : A \to M_X^U(A)$ by $i(a)(x) = x.a$. The induced map on cohomology is the restriction map, res: $H^q(X, A) \to H^q(U, A)$. Similarly, if U is open in X, define the X-module homomorphism

$$\pi : M_X^U(A) \to A, \quad f \mapsto \sum_{\sigma \in X/U} \sigma.f(\sigma^{-1}).$$

This definition is independent of the choice of coset representatives σ of U in X, and induces on cohomology the corestriction map, cor: $H^q(U, A) \to H^q(X, A)$.

Lemma 3.1. (i) *Let U be an open subgroup of X, and let A be an X-module. Then* $\text{cor} \circ \text{res}(\alpha) =$ $[X : U]\alpha$ *for* $\alpha \in H^q(X, A)$.

(ii) *Suppose in addition that U is normal in X with quotient group G. Then* $\text{res} \circ \text{cor}(\alpha) = Sp_G\alpha$ *for any* $\alpha \in H^q(U, A)$. *Here* $Sp_G = \sum_{\sigma \in G} \sigma$ *is the norm element in the group ring* $\mathbf{Z}[G]$.

PROOF (i) is well-known. For example, cor ∘ res is the map on cohomology induced by the composition,

$$A \to M_X^U(A) \to A, \qquad \pi \circ i(a) = \sum_{\sigma \in X/U} \sigma.i(a)(\sigma^{-1}) = [X : U]a.$$

(ii)res ∘ cor is the map induced on cohomology by the composition $M_X^U(A) \to A \to M_X^U(A)$,

$$\begin{aligned} i(\pi(f)(x) = x \sum_{\sigma\in X/U} \sigma.f(\sigma^{-1}) &= \sum_{\sigma\in X/U} x.\sigma.f(\sigma^{-1}) \\ &= \sum_{\sigma\in X/U} \sigma.f(\sigma^{-1}x) \\ &= \sum_{\sigma\in X/U} (\sigma.f)(x) \\ &= Sp_G.f(x). \end{aligned}$$

The result is now immediate in dimension 0, and by dimension-shifting, we obtain the result in general.◇

Let A, B, and C be X-modules. An X-pairing is a $\mathbb{Z}$-bilinear map $\langle -,- \rangle: A \times B \to C$ such that for all $x \in X$, $a \in A$, and $b \in B$, $\langle x.a, x.b\rangle = x.\langle a, b\rangle$. For all $m, n \geq 0$, one obtains a bilinear pairing,

$$- \cup - : H^m(X, A) \times H^n(X, B) \to H^{m+n}(X, C),$$

called the cup-product, defined on cochains by

$$(f \cup g)(x_1, \dots, x_{m+n}) = \langle f(x_1, \dots, x_n), x_1 x_2 \dots x_n.g(x_{n+1}, \dots, x_{m+n})\rangle.$$

Proposition 3.1. *The cup-product has the following properties:*

(i) $\mathrm{res}(f \cup g) = \mathrm{res}(f) \cup \mathrm{res}(g)$;

(ii) $\mathrm{cor}(f \cup \mathrm{res}(g)) = \mathrm{cor}(f) \cup g$;

(iii) $f \cup g = (-1)^{mn} g \cup f$;

(iv) If one has exact sequences $0 \to A_1 \to B_1 \to C_1 \to 0$, $0 \to A_2 \to B_2 \to C_2 \to 0$, $0 \to A_3 \to B_3 \to C_3 \to 0$, *and X-pairings:* $B_1 \times B_2 \to B_3$, $C_1 \times C_2 \to C_3$, $A_1 \times C_2 \to A_3$, $C_1 \times A_2 \to A_3$, *then for* $f \in H^m(X, C_1)$ *and* $g \in H^n(X, C_2)$, *one has*

$$\delta(f \cup g) = \delta(f) \cup g + (-1)^m f \cup \delta(g),$$

where the δ *'s are the appropriate connecting homomorphisms;*

(v) Let X and Y be profinite groups, and let $\langle -,- \rangle_1: A_1 \times A_2 \to A_3$ *(respectively,* $\langle -,- \rangle_2: B_1 \times B_2 \to B_3$*) be an X-pairing (resp., a Y-pairing). If* $\phi: Y \to X$ *and* $\psi_i: A_i \to B_i$ *are such that the pairs* (ϕ, ψ_i) *are compatible, and if for all* $a_1 \in A_1$ *and* $a_2 \in A_2$ *one has*

$$\psi_3(\langle a_1, a_2\rangle_1) = \langle \psi_1(a_1), \psi_2(a_2)\rangle_2, \tag{3.1}$$

then for all $f \in H^m(X, A_1)$ and $g \in H^n(X, A_2)$, one has

$$\psi_1^*(f) \cup \psi_2^*(g) = \psi_3^*(f \cup g),$$

where ψ_i^* is the map induced on cohomology by the map ψ_i.

PROOF (i)–(iii) can be found in [S 2], (iv) is theorem 9 of [Sh 1], and (v) is Sats 3.26 of [Ko 2].◇

As a particular case of (v), consider the X-pairing $A_1 \times A_2 \rightarrow A_3$ to be a U-pairing by restriction, where U is a normal subgroup of X with quotient G. The maps $(\phi_x, \psi_{i,x})$ which induce the natural action of G on $H^n(U, A_i)$, satisfy the condition (3.1), so that the cup-product defines a G-invariant bi-additive form.

One says that the profinite group X has cohomological p-dimension equal to n ($cd_p(X) = n$) if for all torsion modules A and all $m > n$, the p-primary part of the group $H^m(X, A) = 0$, and the p-primary part of $H^n(X, A) \neq 0$ for some such A. The strict cohomological p-dimension of X is n ($scd_p(X) = n$) if the above statement holds for all discrete (not necessarily torsion) X-modules.

Proposition 3.2. *If $cd_p(X) = n < \infty$, then $scd_p(X) = n$ if and only if $H^n(U, \mathbb{Q}/\mathbb{Z}) = 0$ for all open subgroups U of X.*

PROOF See [B 1], cor 5.5.◇

Let X be a profinite group, and let U be a subgroup of finite index. Let $\mathcal{R}$ be a system of left-coset representatives of X/U, and given any $x \in X$; define $\tilde{x} \in \mathcal{R}$ to be the particular coset representative of x: $\tilde{x}^{-1}x \in U$. Define the group-theoretic transfer Ver: $X^{ab} \rightarrow U^{ab}$ by

$$\mathrm{Ver}(x) = \prod_{r \in \mathcal{R}} \widetilde{xr}^{-1} xr \mod [U, U]$$

where $[U, U]$ is the commutator subgroup of U. By Sats 3.12 of [Ko 2], the transfer is dual to the correstriction,

$$\mathrm{cor}: H^1(U, \mathbb{Q}/\mathbb{Z}) \rightarrow H^1(X, \mathbb{Q}/\mathbb{Z}).$$

Proposition 3.3. *Let X be a profinite group with $scd_p(X) = 2$, and let U be a normal subgroup of X with quotient group G. Then the transfer map Ver: $X^{ab} \rightarrow (U^{ab})^G$ is an isomorphism.*

PROOF See [H 1], propositions 10 and 11.◇

§ 3.2 A Demuškin group X is a pro-p group satisfying the following axioms:

(i) $\dim_{\mathbb{F}_p} H^1(X, \mathbb{Z}/p\mathbb{Z}) = n < \infty$;

(ii) $\dim_{\mathbb{F}_p} H^2(X, \mathbb{Z}/p\mathbb{Z}) = 1$;

(iii) The bilinear form on the $\mathbb{F}_p$-vector space $H^1(X, \mathbb{Z}/p\mathbb{Z})$ given by the cup-product is nondegenerate.

With the exception of the trivial case $p = 2$ and $n = 1$, these axioms suffice to show that $cd_p(X) = 2$ (see [S 3]). For any discrete X-module A, define the $\mathbb{Q}/\mathbb{Z}$-dual of A by $A^* = \mathrm{Hom}(\mathrm{A}, \mathbb{Q}/\mathbb{Z})$, carrying the X-action: $(x.f)(a) = f(x^{-1}.a)$. For X of cohomological dimension 2, one defines the "dualizing module" of X,

$$I_X = \varinjlim \varinjlim H^2(U, \mathbb{Z}/p^s\mathbb{Z})^*, \qquad (3.2)$$

where the direct limit is taken over all open subgroups U of X (the maps being the dual of cor) and all $s \geq 1$ (the maps being dual to those induced on cohomology by the projections $\mathbb{Z}/p^s\mathbb{Z} \to \mathbb{Z}/p^r\mathbb{Z}$ for $s \geq r$). It is known (see [S 2], proposition 30) that if A is any p-primary torsion X-module, then $H^2(X, I_X) \cong \mathbb{Q}_p/\mathbb{Z}_p$, and the cup-product

$$H^i(X, A) \times H^{2-i}(X, \mathrm{Hom}(\mathrm{A}, \mathrm{I})) \longrightarrow \mathrm{H}^2(\mathrm{X}, \mathrm{I})$$

is a "perfect pairing" for $0 \leq i \leq 2$, giving the isomorphisms,

$$H^i(X, A)^* \cong H^{2-i}(X, \mathrm{Hom}(\mathrm{A}, \mathrm{I})).$$

As an Abelian group, I_X is isomorphic to $\mathbb{Q}_p/\mathbb{Z}_p$, with X-action given by a homomorphism

$$\chi : X \to \mathrm{Aut}(\mathbb{Q}_p/\mathbb{Z}_p) \cong \mathbb{Z}_p^\times, \quad x.\alpha = \chi(x)\alpha \quad \text{for all } x \in X \text{ and } \alpha \in I_X.$$

χ will be called the invariant of the group X. If the image of χ is infinite, then $scd_p(X) = 2$ (see [S 2], pg. I-52), and it is shown in [L 1] that this image, together with the rank $n = \dim_{\mathbb{F}_p} H^1(X, \mathbb{F}_p)$ of X, form a complete set of invariants for X, determining X uniquely up to isomorphism. For the remainder of this paper, unless otherwise stated we will assume that $scd_p(X) = 2$.

Proposition 3.4. *Let U be an open subgroup of the Demuškin group X. Then one has,*

(i) $I_U = I_X$;

(ii) $H^2(U,\mathbb{Z}/p^s\mathbb{Z})^\times \cong {}_{p^s}U^{ab}$, *where for any Abelian group A, ${}_qA$ is the subgroup of A of exponent q;*

(iii) The torsion submodule $\mathrm{tor}(U^{ab})$ *of U^{ab} is isomorphic to I_X^U, and if U is normal in X with quotient G, then this isomorphism is as G-modules.*

PROOF (i) follows from the definition of the dualising module, since to find I_U one tosses out at most a finite number of terms in the inductive limit (3.2). For (ii), consider the long exact sequence obtained from the exact sequence of U-modules (with trivial action), $0 \to \mathbb{Z}/p^s\mathbb{Z} \to \mathbb{Q}_p/\mathbb{Z}_p \xrightarrow{p^s} \mathbb{Q}_p/\mathbb{Z}_p \to 0$:

$$0 \to H^1(U,\mathbb{Z}/p^s\mathbb{Z}) \to H^1(U,\mathbb{Q}_p/\mathbb{Z}_p) \xrightarrow{p^s} H^1(U,\mathbb{Q}_p/\mathbb{Z}_p) \to H^2(U,\mathbb{Z}/p^s\mathbb{Z}),$$

where the last map is surjective by proposition 3.2 since the $scd_pU = 2$. Taking duals, we obtain the exact sequence,

$$0 \to H^2(U,\mathbb{Z}/p^s\mathbb{Z})^* \longrightarrow U^{ab} \xrightarrow{p^s} U^{ab}, \tag{3.3}$$

where we have identified $H^1(U,\mathbb{Q}_p/\mathbb{Z}_p)^*$ with U^{ab}. Note that for s large enough, we have

$$H^2(U,\mathbb{Z}/p^s\mathbb{Z})^* \cong \mathrm{tor}(U^{ab}).$$

From the commutative diagram (with exact rows),

$$\begin{tikzcd}
0 \arrow[r] & \mathbb{Z}/p^r\mathbb{Z} \arrow[r] & \mathbb{Q}_p/\mathbb{Z}_p \arrow[r, "p^r"] & \mathbb{Q}_p/\mathbb{Z}_p \arrow[r] & 0 \\
0 \arrow[r] & \mathbb{Z}/p^s\mathbb{Z} \arrow[r] \arrow[u, "\mathrm{mod}\ p^r"'] & \mathbb{Q}_p/\mathbb{Z}_p \arrow[r, "p^s"] \arrow[u, "p^{s-r}"'] & \mathbb{Q}_p/\mathbb{Z}_p \arrow[r] \arrow[u, equal] & 0
\end{tikzcd}$$

we obtain (after dualising) the commutative diagram (with exact rows),

$$\begin{tikzcd}
0 \arrow[r] & H^2(U,\mathbb{Z}/p^s\mathbb{Z})^* \arrow[r] & U^{ab} \arrow[r] & U^{ab} \\
0 \arrow[r] & H^2(U,\mathbb{Z}/p^r\mathbb{Z})^* \arrow[r] \arrow[u] & U^{ab} \arrow[r] \arrow[u, equal] & U^{ab} \arrow[u]
\end{tikzcd} \tag{3.4}$$

and a little diagram-chasing shows that $H^2(U,\mathbb{Z}/p^r\mathbb{Z})^* \to H^2(U,\mathbb{Z}/p^s\mathbb{Z})^*$ is injective. Now if $V \leq U$ is open, and $V_0 \leq V$ is normal in U with quotient G, then by proposition 3.3, $\mathrm{Ver}\colon U^{ab} \to (V_0{}^{ab})^G$ is an isomorphism; the transitivity of the transfer map implies that Ver "factors through" V^{ab}, so that $U^{ab} \to V^{ab}$ is injective. It follows that

$$H^2(U,\mathbb{Z}/p^s\mathbb{Z})^* \to H^2(V,\mathbb{Z}/p^s\mathbb{Z})^*$$

is injective for all s, and hence all the maps in (3.2) are injective. In particular, by choosing s large enough we obtain the injection $\mathrm{tor}(U^{ab}) \to I_X^U$. Let $V \leq X$ be the stabliser of I_X^U, so that $I_X^U = I_X^V$. Since $U \leq V$, and the composition $\mathrm{tor}(V^{ab}) \to \mathrm{tor}(U^{ab}) \to I_X^V$ is injective, it suffices to prove (iii) for V. If s is a generator of I_X^V (as an Abelian group) "coming from" $H^2(W, \mathbb{Z}/p^s\mathbb{Z})^*$ for some open normal subgroup W of V in the direct limit (3.2), then $s \in \mathrm{tor}(W^{ab})^V$. But by proposition 3.3, $V^{ab} \to (W^{ab})^V$ is an isomorphism, so that $s \in V^{ab}$ already.◇

The order q of the torsion submodule of X^{ab} is called the torsion invariant of the Demuškin group X. In view of the above proposition, q is determined by the image in $\mathbb{Z}_p^\times$ of the invariant χ: if $s \in I_X$ has order q, then for $x \in X$, $x.s = \chi(x)s = s$ if and only if $\chi(x) \equiv 1 \pmod{q}$.

Proposition 3.5. *With notation as above, one has the following description of* $\mathrm{im}(\chi)$*:*

(i) If $p \neq 2$*, then* $\mathrm{im}(\chi)$ *is of the form* $1 + p^s\mathbb{Z}_p$ *for some* $s \geq 1$ *,and the torsion invariant is* $q = p^s$*;*

If $p = 2$*, there are three possibilities for* $\mathrm{im}(\chi)$*:*

(ii) $\mathrm{im}(\chi) = \{\pm 1\} \times \{1 + 2^s\mathbb{Z}_2\}$ *with* $s \geq 2$*, and the torsion invariant* q *is* 2*;*

(iii) $\mathrm{im}(\chi) = 1 + 2^s\mathbb{Z}_2$ *with* $s \geq 2$*,and* $q = 2^s$*;*

(iv) $\mathrm{im}(\chi)$ *is the subgroup of* ${\mathbb{Z}_2}^\times$ *generated (as a free* $\mathbb{Z}_p$*-module) by* $-1 + 2^s$ *with* $s \geq 2$*, and* $q = 2$*.*

PROOF These are the only infinite subgroups of $\mathbb{Z}_p^\times$.◇

Corollary. *The Demuškin group* X *contains a unique subgroup* U *(the "cyclotomic subgroup") of index* p *having torsion invariant strictly greater that that of* X*.*

PROOF If $\mathrm{im}(\chi)$ is as in (i), (iii), or (iv) above, take $U = \chi^{-1}(1 + p^{s+1}\mathbb{Z}_p)$, while in (ii) let $U = \chi^{-1}(1 + 2^s\mathbb{Z}_2)$. The uniqueness is clear.◇

§ 3.6 In [S 3] and [L 1] a method is given to compute the invariant χ of the Demuškin group X explicitly from a given minimal presentation of X. We develop below a more "geometric" method to find the cyclotomic subgroup.

We first remark that if the torsion invariant of X is q, then

$$H^1(X, \mathbb{Z}/q\mathbb{Z}) \times H^1(X, \mathbb{Z}/q\mathbb{Z}) \xrightarrow{\cup} H^2(X, \mathbb{Z}/q\mathbb{Z}) \tag{3.5}$$

is a non-degenerate form. Indeed, if we let π_i denote the (surjective!) maps on the i^{th} cohomology groups induced by the surjection $\mathbb{Z}/q\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$, then $\pi_1(f) \cup \pi_1(g) = \pi_2(f \cup g)$ (this follows from proposition 3.1 (v)). If $\psi_1 \in H^1(X, \mathbb{Z}/q\mathbb{Z})$ has order q, then $\pi_1(\psi_1) \neq 0$, so there is a $\pi_1(\psi_2)$ such that

$$\pi_1(\psi_1) \cup \pi_1(\psi_2) = \pi_2(\psi_1 \cup \psi_2) \neq 0,$$

and $\psi_1 \cup \psi_2$ has order q. The claim now follows from the $\mathbb{Z}/q\mathbb{Z}$-linearity of the cup product.

Let X have torsion invariant $q = p^e$, and consider the long exact sequence associated to the exact sequence $0 \to {}_qI_X \to {}_{q^2}I_X \xrightarrow{q} {}_qI_X \to 0$:

$$0 \to H^0(X, {}_qI_X) \to H^0(X, {}_{q^2}I_X) \to H^0(X, {}_qI_X) \xrightarrow{\delta} H^1(X, {}_qI_X) \to \ldots,$$

from which one obtains the injection ${}_qI_X \to H^1(X, {}_qI_X)$ given by the connecting homomorphism δ. Let s be a generator of ${}_qI_X$, and let $\theta = \delta(s)$. If $w \in {}_{q^2}I_X$ is such that $q.w = s$, then for $x \in X$,

$$\theta(x) = \delta(s)(x) = x.w - w.$$

Since w is a generator of ${}_{q^2}I_X$, $U = \ker(\theta)$ is the unique subgroup of X of index q fixing ${}_{q^2}I_X$, so that $p^{e-1}\theta = \theta_0$ will have the cyclotomic subgroup as its kernel. Using this choice of generator $s \in {}_qI_X$, we may identify ${}_qI_X$ with $\mathbb{Z}/q\mathbb{Z}$ by $s \leftrightarrow 1$; we may thus think of θ as an element of $H^1(X, \mathbb{Z}/q\mathbb{Z})$.

The "Bockstein operator" $B: H^1(X, \mathbb{Z}/q\mathbb{Z}) \to H^2(X, \mathbb{Z}/q\mathbb{Z})$ is the connecting homorphism coming from the sequence $0 \to \mathbb{Z}/q\mathbb{Z} \to \mathbb{Z}/q^2\mathbb{Z} \xrightarrow{q} \mathbb{Z}/q\mathbb{Z} \to 0$. An explicit calculation of this connecting homorphism shows that

$$\ker(B) = \{\psi \in H^1(X, \mathbb{Z}/q\mathbb{Z}) \text{ such that } \psi(x) = 0 \text{ for } x \in tor(X^{ab})\}.$$

Proposition 3.6. *The one dimensional subspace* $\ker(B)^{\perp}$ *of* $H^1(X, \mathbb{Z}/q\mathbb{Z})$ *is the subspace generated by the character* θ *defined above (where the inner product is given by the cup-product as in (3.5) above).*

PROOF From proposition 6 of [L 1], it is known that the map $H^1(X, {}_{q^2}I_X) \to H^1(X, {}_pI_X)$ is surjective; since this map "factors through" $H^1(X, {}_qI_X)$, and since q is the torsion-invariant of X, we may conclude that the map $H^1(X, {}_{q^2}I_X) \to H^1(X, {}_qI_X)$ is also surjective. It follows that the connecting homomorphism $\delta \colon H^1(X, {}_qI_X) \to H^2(X, {}_qI_X)$ in the long exact sequence associated to the exact sequence $0 \to {}_qI_X \to {}_{q^2}I_X \to {}_qI_X \to 0$ is the zero map. From the G-pairings ${}_qI_X \times \mathbb{Z}/q\mathbb{Z} \to {}_qI_X$ and ${}_{q^2}I_X \times \mathbb{Z}/q^2\mathbb{Z} \to {}_{q^2}I_X$, we thus have the commutative diagram (see proposition 3.1 (iv)),

$$\begin{tikzcd}
H^1(X, {}_qI_X) \arrow[r, phantom, "\times"] & H^1(X, \mathbb{Z}/q\mathbb{Z}) \arrow[r, "\cup"] \arrow[d, "B"] & H^2(X, {}_qI_X) \arrow[d, equal] \\
H^0(X, {}_qI_X) \arrow[u, "-\theta"] \arrow[r, phantom, "\times"] & H^2(X, \mathbb{Z}/q\mathbb{Z}) \arrow[r, "\cup"] & H^2(X, {}_qI_X)
\end{tikzcd} \tag{3.6}$$

It follows that the subgroup generated by θ is contained in $\ker(B)^{\perp}$; but $\ker(B)$ has co-dimension 1 in $H^1(X, \mathbb{Z}/q\mathbb{Z})$. The cup-product is nondegenerate, so $\ker(B)^{\perp}$ is one-dimensional, hence generated by θ.◇

§ 3.4. **Examples** . (1) If X has (even) rank n and torsion invariant $q \neq 2$, then by [S 3] there exists a minimal generating set $x_1, \ldots, x_n$ of X satisfying the defining relation

$$1 = x_1{}^q[x_1, x_2] \ldots [x_{n-1}, x_n],$$

and the invariant $\chi \colon X \to \mathbb{Z}_p^{\times}$ is given by

$$\chi(x_i) = \begin{cases} 1; & \text{if } i \neq 2; \\ (1+q)^{-1}, & i = 2. \end{cases}$$

If $\psi_1, \ldots, \psi_n \in H^1(X, \mathbb{Z}/q\mathbb{Z})$ is the dual basis of the images $\bar{x}_1, \ldots, \bar{x}_n$ of the x_i's in $X/X^q[X, X]$, then

$$Y = \ker(\psi_2) = \chi^{-1}(1 + q^2\mathbb{Z}_p)$$

is the unique subgroup of X of index q having torsion invariant q^2.

(2) If the torsion invariant of X is 2 and the generating rank n is odd, (again, [S 3]) there exist generators x_i satisfying the defining relation

$$1 = x_1{}^2x_2{}^{2^s}[x_2, x_3] \ldots [x_{n-1}, x_n]$$

with $s \geq 2$. In this case, χ is given by

$$\chi(x_i) = \begin{cases} -1, & i = 1, \\ 1 + 2^s, & i = 2, \\ 1, & \text{otherwise}; \end{cases}$$

the cyclotomic subgroup is

$$Y = \ker(\psi_1) = \chi^{-1}(1 + 2^s\mathbb{Z}_2),$$

and the torsion invariant of Y is 2^s.

(6) If the torsion invariant of X is 2 and the rank n is even, there exist generators x_i for which a defining relation can be found of one of the following two forms (see [L 1]):

$$1 = x_1^2[x_1, x_2]x_2^{2^s}[x_3, x_4]\dots[x_{n-1}, x_n], \tag{3.7}$$

$$1 = x_1^{2+2^s}[x_1, x_2][x_3, x_4]\dots[x_{n-1}, x_n], \tag{3.8}$$

with $s \geq 2$ in both cases. The values of the invariant are given by,

$$\chi(x_i) = \begin{cases} -1, & i = 2; \\ (1 + 2^s)^{-1}, & i = 4; \\ 1, & \text{otherwise}, \end{cases} \tag{3.7'}$$

$$\chi(x_i) = \begin{cases} (-1 - 2^s), & i = 2; \\ 1, & \text{otherwise}. \end{cases} \tag{3.8'}$$

In case (5), the cyclotomic subgroup

$$Y = \ker(\psi_2) = \chi^{-1}(1 + 2^s\mathbb{Z}_2)$$

has torsion invariant 2^s, while in (6)

$$Y = \ker(\psi_2) = \chi^{-1}(1 + 2^{s+1}\mathbb{Z}_2)$$

has torsion invariant 2^{s+1}.

Note that in each of the above examples, the character θ whose kernel is the cyclotomic subgroup Y, can be determined (as in proposition 3.6) as a generator of $\ker(B)^{\perp}$. For example, if X is the Demuškin group determined by relation (3.7),

$$\ker(B) = \{\psi \in H^1(X, \mathbb{Z}/2\mathbb{Z}) : \psi(s) = 0 \text{ for } s \in \operatorname{tor}(X^{ab})\} = \langle \psi_2, \dots, \psi_n \rangle,$$

and the perpendicular complement of this subspace of $H^1(X, \mathbb{Z}_2)$ is $\langle \psi_2 \rangle$.

Remark. If the $scd_p(X) \neq 2$, the result of prop. 3.3 is no longer valid. For example, let X be minimally generated by x_1, x_2, x_3 with the defining relation

$$1 = x_1^2[x_2, x_3].$$

A calculation as in [L 1] shows that the invariant χ is defined by

$$\chi(x_i) = \begin{cases} -1, & i = 1, \\ 1, & \text{otherwise}, \end{cases}$$

and the image of χ in $\mathbb{Z}_2^\times$ is $\{\pm 1\}$. By [S 2] it follows that $scd_2(X) = 3$. Now $\ker(B)$ is the subspace generated by χ_2 and χ_3, and its perpendicular complement is the subspace generated by χ_1. One can show that $(\ker(\chi_1))^{ab}$ is torsion-free.

§ 3.5. It is well-known (see [S 3]) that any open subgroup of a Demulkin group is again a Demulkin group. If $U \subset X$ is open with index $|X : U|$, then the generating rank of U can be calculated using "Euler-Poincaré characteristics" (e.g.,[Ko 2], § 5.2):

$$\chi_U = |X : U|\chi_X \qquad \text{where} \quad \chi_Y = \sum_{n=0}^{\infty}(-1)^n \dim_{\mathbb{F}_p} H^n(Y, \mathbb{Z}/p\mathbb{Z}),$$

for any pro-p group Y of finite cohomological dimension. If X is minimally generated by $n+2$ elements, then $\chi_X = 1 - (n+2) + 1 = n$, we have $\chi_U = n|X : U|$, and hence U has generating rank $n|X : U| + 2$.

Proposition 3.7. *Let X be a Demulkin p-group with $scd_p X = 2$, and let $\omega \in H^1(X, \mathbb{Z}/p\mathbb{Z})$. If $Y = \ker(\omega)$, then one has the exact sequence,*

$$H^1(Y, \mathbb{Z}/p\mathbb{Z}) \xrightarrow{cor} H^1(X, \mathbb{Z}/p\mathbb{Z}) \xrightarrow{\cup\omega} H^2(X, \mathbb{Z}/p\mathbb{Z}) \to 0.$$

PROOF From proposition 3.1 (ii), we have the commutative diagram,

$$\begin{tikzcd} H^1(X, \mathbb{Z}/p\mathbb{Z}) \arrow[d, "res"] & \times & H^1(X, \mathbb{Z}/p\mathbb{Z}) & \longrightarrow & H^2(X, \mathbb{Z}/p\mathbb{Z}) \\ H^1(Y, \mathbb{Z}/p\mathbb{Z}) & \times & H^1(Y, \mathbb{Z}/p\mathbb{Z}) \arrow[u, "cor_1"] & \longrightarrow & H^2(Y, \mathbb{Z}/p\mathbb{Z}), \arrow[u, "cor_2"] \end{tikzcd} \tag{3.9}$$

where cor_2 is an isomorphism by proposition 3.4. Let $W = \mathrm{im}(cor_1)$; given any $\theta \neq \omega$ in W, there is a $\phi \in H^1(Y, \mathbb{Z}/p\mathbb{Z})$ such that $1 = res\theta \cup \phi = \theta \cup cor\phi$, so that either W is a complete subspace of

$H^1(X, \mathbb{Z}/p\mathbb{Z})$, or the radical of W is $\langle\omega\rangle$. If the former case, let $\psi \in W^{\perp}$, and suppose that $\psi \notin \langle\omega\rangle$. As above, we can find a ϕ such that $\mathrm{res}\psi \cup \phi = 1$, and hence that $\psi \cup \mathrm{cor}\phi = 1$, a contradiction. It follows in this case that $H^1(X, \mathbb{Z}/p\mathbb{Z}) = W \perp \langle\omega\rangle$ as complete spaces, and hence that $W = \ker(\omega)^{\perp}$. If ω generates the radical of W, choose $\eta \in H^1(X, \mathbb{Z}/p\mathbb{Z})$ so that $\eta \cup \omega = 1$; then W and η generate a complete subspace of $H^1(X, \mathbb{Z}/p\mathbb{Z})$ which must be the whole space by arguing as above. Thus in this case also, $W = \ker(\mathrm{cor})$. The surjectivity of $\cdot \cup \omega$ is clear from the non-degeneracy of the cup-product. ◇

Corollary. *Let X be a Demuškin 2-group, and let $\omega \in H^1(X, \mathbb{Z}/2\mathbb{Z})$. Letting $Y = \ker(\omega)$ and $\Delta = X/Y$, one has the following exact sequence:*

$$0 \to H^1(\Delta, \mathbb{Z}/2\mathbb{Z}) \xrightarrow{\mathrm{inf}} H^1(X, \mathbb{Z}/2\mathbb{Z}) \xrightarrow{\mathrm{res}} H^1(Y, \mathbb{Z}/2\mathbb{Z}) \xrightarrow{\mathrm{cor}} H^1(X, \mathbb{Z}/2\mathbb{Z}) \xrightarrow{\cdot\cup\omega} H^2(X, \mathbb{Z}/2\mathbb{Z}) \to 0.$$

PROOF Exactness at the first $H^1(X, \mathbb{Z}/2\mathbb{Z})$ follows from the Hochschild–Serre spectral sequence (see, for example, Satz 3.15 of [Ko 2]) and at the second $H^1(X, \mathbb{Z}/2\mathbb{Z})$ from proposition 3.4 above. Since $\mathrm{cor} \circ \mathrm{res} : H^1(X, \mathbb{Z}/2\mathbb{Z}) \to H^1(X, \mathbb{Z}/2\mathbb{Z})$ is the zero-map, $\mathrm{im}(\mathrm{res}) \subset \ker(\mathrm{cor})$. On the other hand, if the generating rank of X is $n+2$, $\mathrm{im}(\mathrm{cor})$ has rank $n+1$, so that $\ker(\mathrm{cor})$ has rank $2n+2-(n+1) = n+1$ from the above computation with Euler-Poincaré characteristics. This is the rank of $\mathrm{im}(\mathrm{res})$, giving exactness at the middle term.◇

Chapter 4. $\mathbf{Z}_p$-Towers in Demuškin Groups

In this chapter, we define the notion of a $\mathbf{Z}_p$-tower in a Demuškin group. When $p \neq 2$ and when $p = 2$ and the "torsion-invariant of the tower" is not 2, we obtain a complete classification of these towers. When the torsion-invariant of the tower is 2, a complete classification is not obtained, but we examine some necessary invariants. § 4.1 Let X be a Demuškin group with $scd_p X = 2$. By the $\mathbf{Z}_p$-tower (X, ϕ) we shall mean a (continuous) epimorphism $\phi : X \to \mathbf{Z}_p$ of X onto the additive group of p-adic integers. Two such towers (X, ϕ_1) and (Y, ϕ_2) are said to be isomorphic if there is an isomorphism $\alpha : X \to Y$ so that $\phi_1 = \phi_2 \circ \alpha$. For a fixed tower (X, ϕ), define the n^{th} level subgroup $X_n = \phi^{-1}(p^n \mathbf{Z}_p)$, so that $X = X_0 \supset X_1 \supset \dots$ gives a chain of normal subgroups of X with $X/X_n = G_n \cong \mathbf{Z}/p^n\mathbf{Z}$, and $\cap X_n = V$ is the kernel of ϕ.

$\mathbf{Z}_p$ towers in a given Demuškin group are quite plentiful: any non trivial element of $\text{Hom}(X, \mathbf{Z}_p)$ will define one. If X has torsion invariant q and is minimally generated by n elements, then $X^{ab} \cong \mathbf{Z}/q\mathbf{Z} \oplus \mathbf{Z}_p{}^{n-1}$, so that $\text{Hom}(X, \mathbf{Z}_p)$ is a free $\mathbf{Z}_p$-module of rank $n - 1$. An example of particular interest is the "basic tower": if χ is the invariant of X, then for each of the possible images of χ listed in proposition 3.5, there is a unique (up to choice of topological generator) surjection π of $\text{im}(\chi)$ onto $\mathbf{Z}_p$; the composition $\phi = \pi \circ \chi$ will yield a $\mathbf{Z}_p$ tower in X. In fact, if $\text{im}(\chi) \neq \{\pm 1\} \times \{1 + 2^e \mathbf{Z}_2\}$, then $\text{im}(\chi)$ is already isomorphic to $\mathbf{Z}_p$, while in the remaining case, projection onto the second factor gives a suitable π. The object of this chapter is to classify isomorphism classes of towers in the following sense: Let Υ be the group of continuous automorphisms of X; then Υ acts on the space $\text{Hom}(\text{X}, \mathbf{Z}_p)$ by

$$(v.\phi)(x) = \phi(v.x),$$

where $v \in \Upsilon$, $\phi \in \text{Hom}(\text{X}, \mathbf{Z}_p)$, and $x \in X$. The orbits under this action will be our equivalence classes, and we will endeavor to give invariants which distinguish orbits.

Lemma 4.1. *The chain of subgroups X_n in the basic tower is invariant under all automorphisms of X.*

PROOF Successively find the cyclotomic subgroups Y_1 of X, Y_2 of Y_1, etc., whose existence and uniqueness at each stage is guaranteed by the corollary to proposition 3.5. The uniqueness implies that each Y_i is a characteristic subgroup of Y_{i-1}, and hence characteristic in X. It follows that $\cap Y_i = V = \ker\chi$ is characteristic in X. If $\mathrm{im}(\chi) \cong \mathbb{Z}_p$, we are done. If $\mathrm{im}(\chi) \cong \mathbb{Z}_2 \oplus \mathbb{Z}/2\mathbb{Z}$, then $V_0 = \chi^{-1}(\mathbb{Z}/2\mathbb{Z})$ is characteristic in X: this follows because V is characteristic in X and V_0/V, being the torsion subgroup of X/V, is characteristic. The X_i are the level subgroups in the tower given by X/V_0, and since X_i/V_O is characteristic in X/V_0, X_i is characteristic in X.◇

If (X, ϕ) is a $\mathbb{Z}_p$-tower which is not the basic tower, there is a maximal positive integer n_0 such that the $n_0{}^{th}$ level subgroup X_{n_0} is the same as the $n_0{}^{th}$ level subgroup in the basic tower. That is, letting $V = \ker(\phi)$, there is an integer $q = p^s$ and an integer n_0 such that for all $n \geq n_0$,

$$\mathrm{tor}(X_n^{ab}) \cong I_X^V \cong \mathbb{Z}/p^s\mathbb{Z}$$

as Abelian groups. We will call this q the torsion invariant *of the tower* (X, ϕ). If $q \neq 2$, define the homomorphism $\alpha: \mathbb{Z}_p \longrightarrow (\mathbb{Z}/q\mathbb{Z})^\times$ which gives the action of $X/V \cong \mathbb{Z}_p$ on I_X^V: for any $\varsigma \in I_X^V$, $x \in X$, and $\bar{x}$ the image of x in X/V,

$$x.\varsigma = \bar{x}.\varsigma = \alpha(\bar{x})\varsigma.$$

In view of lemma 4.1, the integer q and the image of α in $\mathbb{Z}/q\mathbb{Z}^\times$ will be left unchanged under the action of any continuous automorphism of X. Proposition 4.2 below shows that, in the case where $q \neq 2$, the classes of towers are distinguished by q and α.

§ 4.2 The key ingredient in showing that the invariants q and α defined in the previous section determine the tower (X, ϕ) up to isomorhism, is the notion (due to Koch, [Ko 4]) of the so-called "Demuškin formation over G" having specified parameters, which we describe below.

Let $\mathcal{G}'$ be the profinite group generated by elements σ and τ, subject to the single relation:

$$\sigma\tau\sigma^{-1} = \tau^{p^f},$$

and let $\mathcal{G}$ be any p-closed quotient thereof (i.e., any quotient divisible by p^∞). Let $n, s \geq 1$ be integers, and let $\alpha: \mathcal{G} \longrightarrow (\mathbb{Z}/p^s\mathbb{Z})^\times$ be a continuous homomorphism. A Demuškin formation (X, ϕ) over $\mathcal{G}$ with invariants n,s, and α is a surjective homomorphism $\phi: X \to \mathcal{G}$ of topological groups, with pro-p kernel

V, satisfying axioms (1), (2), and (3) below. With $\mathcal{N} \triangleleft \mathcal{G}$, $\mathcal{N} \subset \ker(\alpha)$, $G = \mathcal{G}/\mathcal{N}$, and $X_{\mathcal{N}} = \phi^{-1}(\mathcal{N})$, we suppose:

(1) The maximal pro-p quotient $\tilde{X}_{\mathcal{N}}$ of $X_{\mathcal{N}}$ is a Demuškin group of rank $n|G| + 2$, having torsion invariant p^s;

(2) The symplectic space $H^1(\mathcal{N}, \mathbb{Z}/p\mathbb{Z})^{\perp}/H^1(\mathcal{N}, \mathbb{Z}/p\mathbb{Z})$ is a free $\mathbb{F}_p[G]$-module of rank n, and the bilinear form (induced on this space by the cup product) is hyperbolic: there exists a decomposition of this space into two totally isotropic submodules;

(3) G acts on $H^2(X_{\mathcal{N}}, \mathbb{Z}/p^s\mathbb{Z})^*$ by means of the character α.

Proposition 4.1. *If $p \neq 2$, or if $p = 2$ and $s \geq 2$, any two Demuškin formations over $\mathcal{G}$ having the same invariants $n, s,$ and α are isomorphic.*

PROOF The theorem was first stated for $p \neq 2$ by Koch ([Ko 4]), and proved in detail by Wingberg ([W 1], Satz 1). The case $p = 2$ and $s \geq 2$ was proved by Diekert ([D 1], § 2.2).◇

§ 4.3 Let X be a Demuškin group of scd$_p = 2$ and having generating rank $n + 2$. Suppose that (X, ϕ) is a $\mathbb{Z}_p$-tower which is not the basic tower,let $V = \ker(\phi)$, and suppose that the torsion invariant $q = p^s$ of the tower is not 2. Define $\alpha\colon \mathcal{G} \to \mathbb{Z}/p^s\mathbb{Z}^{\times}$ to be the character giving the action of $\mathcal{G} \cong X/V$ on ${}_qI_X$. If $p^m\mathbb{Z}_p \cong \mathcal{N} \subset \ker(\alpha)$, with $G = \mathcal{G}/\mathcal{N} \cong X/X_m$, then a computatuion using Euler-Poincaré characteristics (see §3.5) shows that $X_m = X_{\mathcal{N}}$ is a Demuškin group of rank $n|G| + 2$ with torsion invariant $q = p^s$, and α gives the action of G on ${}_qI_X \cong H^2(X_{\mathcal{N}}, \mathbb{Z}/q\mathbb{Z})^*$. Thus the tower (X, ϕ) satisfies the first and third axioms for a Demuškin formation over $\mathcal{G} \cong \mathbb{Z}_p$ with invariants n, s, and α.

Define $\phi_m \in H^1(X_m, \mathbb{Z}/p\mathbb{Z})$ by

$$\phi_m(x) = \frac{1}{p^m}\mathrm{res}_{X_m}(\phi)(x) \pmod{p}, \tag{4.1}$$

for $x \in X_m$.

Lemma 4.2. *ϕ_m is fixed under the action of $G = X/X_m$.*

PROOF If $\phi(y) = 1$, then $\{1, y, \ldots, y^{p^m - 1}\}$ is a complete set of coset representatives of X_m in X. Letting $\sigma = \bar{y}$, we have for any $x \in X_m$,

$$\begin{aligned} \phi_m^\sigma(x) = \phi_m(y^{-1}xy) &= \frac{1}{p^m}\phi(y^{-1}xy) \pmod p \\ &= \frac{1}{p^m}\phi(x) \pmod p \qquad (4.2) \\ &= \phi_m(x), \end{aligned}$$

since ϕ vanishes on the commutator $[x, y]$.◇

Lemma 4.3. *The image of ϕ_m under cor: $H^1(X_m, \mathbb{Z}/p\mathbb{Z}) \to H^1(X, \mathbb{Z}/p\mathbb{Z})$ is ϕ_0.*

PROOF From lemma 3.1, res $\circ$ cor$(\phi_m) = Sp_G.\phi_m = |G|\phi_m = 0$, since ϕ_m is fixed by G. On the other hand, ker(res) $= \langle\phi_0\rangle$, so that cor$(\phi_m) = a\phi_0$ for some $a \in \mathbb{Z}/p\mathbb{Z}$, and

$$a = \mathrm{cor}(\phi_m)(y) = \phi_m(\mathrm{Ver}_{X \to X_n}(y)) = \phi_m(\prod_{i=0}^{p^m-1}(\widetilde{yy^i}^{-1}yy^i)) = \phi_m(y^{p^m}) = 1,$$

where $\tilde{x}$ is the coset representative of $x \in X_m$.◇

Consider the following commutative diagram (see proposition 3.1(ii)):

$$\begin{tikzcd} H^1(X_m, \mathbb{Z}/p\mathbb{Z}) & \times & H^1(X_m, \mathbb{Z}/p\mathbb{Z}) \arrow[d, "\mathrm{cor}"] & \arrow[r, "-\cup-"] & H^2(X_m, \mathbb{Z}/p\mathbb{Z}) \arrow[d, "\mathrm{cor}"] \\ H^1(X, \mathbb{Z}/p\mathbb{Z}) \arrow[u, "\mathrm{res}"] & \times & H^1(X, \mathbb{Z}/p\mathbb{Z}) & \arrow[r, "-\cup-"] & H^2(X, \mathbb{Z}/p\mathbb{Z}). \end{tikzcd} \qquad (4.3)$$

The non-degeneracy of the cup-product allows us to choose $\eta \in H^1(X, \mathbb{Z}/p\mathbb{Z})$ so that $\eta \cup \phi_0 = 1$, and the restriction of the cup-product to $V_0 = \langle\phi_0, \eta\rangle^\perp \subset H^1(X, \mathbb{Z}/p\mathbb{Z})$ is a non-degenerate form. From diagram (4.3),

$$\mathrm{res}(\eta) \cup \phi_m = \eta \cup \mathrm{cor}(\phi_m) = \eta \cup \phi_0 = 1,$$

so that $V_m = \langle\phi_m, \mathrm{res}(\eta)\rangle^\perp \subset H^1(X_m, \mathbb{Z}/p\mathbb{Z})$ is a vector space of dimension $n|G|$ with a non-degenerate, G-invariant, alternating form induced by the cup-product.

Lemma 4.4. *cor: $V_m \to V_0$ is surjective.*

PROOF First note that, if $X \supset Y \supset Z$, then cor: $H^1(Z, \mathbb{Z}/p\mathbb{Z}) \to H^1(X, \mathbb{Z}/p\mathbb{Z})$ "factors through" $H^1(Y, \mathbb{Z}/p\mathbb{Z})$—this follows easily from an explicit calculation on cochains. This being the case, it suffices to show that $V_m \xrightarrow{\mathrm{cor}} V_{m-1}$ is surjective. We know by proposition 3.7 that cor: $H^1(X_m, \mathbb{Z}/p\mathbb{Z}) \to$

$H^1(X_{m-1}, \mathbb{Z}/p\mathbb{Z})$ has image equal to $\ker(\cdot \cup \phi_{m-1})$; if $\theta \in V_{m-1}$, choose $\theta' \in H^1(X_m, \mathbb{Z}/p\mathbb{Z})$ such that $\mathrm{cor}(\theta') = \theta$, and write $\theta' = a\phi_m + b\eta + c\gamma$ with a, b, and c in $\mathbb{Z}/p\mathbb{Z}$, and with $\gamma \in V_m$. Because

$$\mathrm{res}\eta \cup \theta' = \eta \cup \mathrm{cor}\theta' = \eta \cup \theta = 0,$$

we know that $a = 0$. Since $\mathrm{cor}(\theta') = \mathrm{cor}(\theta' - b\eta)$, we conclude that $\mathrm{cor}(c\gamma) = \theta$, so that $\mathrm{cor}(V_m) = V_{m-1}$. ◇

Lemma 4.5. *Let $G \cong \mathbb{Z}/p^m\mathbb{Z}$, let M be a finitely-generated $\Lambda = \mathbb{F}_p[G]$-module, and let r be the rank of a maximal free Λ-summand of M. Then r is the $\mathbb{F}_p$-rank of $Sp_G M$, the subspace of "G-norms" in M.*

PROOF $\mathbb{F}_p[G]$ is a local ring having principal maximal ideal generated by the element $\pi = (\sigma - 1)$, where σ is a generator of the cyclic group G. Now every indecomposible $\mathbb{F}_p[G]$-module is isomorphic to some power of the maximal ideal: indeed, since $\mathbb{F}_p[G]$ is the image of the P.I.D. $R = \mathbb{F}_p[T]$, M is a finitely-generated R-module and we may use the structure theorem for finitely-generated modules over a P.I.D. to write

$$M = R^r \oplus \bigoplus_{i=1}^{s} R/(a_i),$$

with $a_i \in R$. Reading this modulo the kernel $(T^{p^m})R$ of the ring epimorphism $R \to \mathbb{F}_p[G]$ induced by $T \mapsto \pi$, we get the structure of M as an $\mathbb{F}_p[G]$-module. In particular, if N is indecomposible, either $N \cong \mathbb{F}_p[G]$ or $N \cong \mathbb{F}_p[G]/(\pi)^b$ for some b. One can check that in the latter case, $N \cong (\pi)^{p^m-b}\mathbb{F}_p[G]$. The Krull-Schmidt theorem holds for finitely-generated $\mathbb{F}_p[G]$-modules, so we may write

$$M \cong \mathbb{F}_p[G]^r \oplus \bigoplus_{i=1}^{s} (\pi)^{b_i}. \tag{4.4}$$

Now $Sp_G = (\pi)^{p^m-1}$ (see lemma 1.3), so if we multiply the equation (4.4) by this element, we obtain $Sp_G.M \cong \mathbb{F}_p[G]^r$, the non-free terms being annihilated.◇

Lemma 4.6. *The space V_m is a free $\mathbb{F}_p[G]$-module of rank n, and as a symplectic space, possesses the "hyperbolic" decomposition: $V_m = W_m \oplus Z_m$, with the submodules W_m and Z_m totally isotropic.*

PROOF From lemma 3.1, $\mathrm{res} \circ \mathrm{cor} = Sp_G$; the restriction map res: $H^1(X, \mathbb{Z}/p\mathbb{Z}) \to H^1(X_m, \mathbb{Z}/p\mathbb{Z})$ is injective on V_0, while cor is surjective, so that the image of $\mathrm{res} \circ \mathrm{cor}\colon V_m \to V_m$ has $\mathbb{F}_p$-rank n. Lemma

4.5 thus assures us of a free $\mathbf{F}_p[G]$-summand of rank n. On the other hand, the $\mathbf{F}_p$-dimension is exactly $n|G|$, so V_m is free as an $\mathbf{F}_p[G]$-module, of rank n. The bilinear form on V_m induced by the cup-product is non-degenerate, V_m being the orthogonal complement of the non-degenerate subspace generated by ϕ_0 and η. This form is also alternating: the cup-product is always anti-symmetric, and so long as $p \neq 2$ this will imply the alternating property (see §1.1). If $p = 2$, we're still alright: since the torsion-invariant of the tower is $q \neq 2$ by hypothesis, the torsion-invariant q' of X_i for $i \geq 1$ is at least 4, and so the cup-product

$$H^1(X_m, \mathbf{Z}/q'\mathbf{Z}) \times H^1(X_m, \mathbf{Z}/q'\mathbf{Z}) \rightarrow H^2(X_m, \mathbf{Z}/q'\mathbf{Z})$$

is nondegenerate. The maps induced on cohomology by the surjection $\mathbf{Z}/q'\mathbf{Z} \rightarrow \mathbf{Z}/2\mathbf{Z}$, give the commutative diagram (see proposition 3.1 (v)),

$$\begin{tikzcd}
H^1(X_m, \mathbf{Z}/q'\mathbf{Z}) \arrow[d] & \times & H^1(X_m, \mathbf{Z}/q'\mathbf{Z}) \arrow[d] \arrow[r] & H^2(X_m, \mathbf{Z}/q'\mathbf{Z}) \arrow[d] \\
H^1(X_m, \mathbf{Z}/2\mathbf{Z}) & \times & H^1(X_m, \mathbf{Z}/2\mathbf{Z}) \arrow[r] & H^2(X_m, \mathbf{Z}/2\mathbf{Z}).
\end{tikzcd}$$

The vertical maps in this diagram are all surjective, being essentially reduction (mod 2). From the anti-symmetry of the cup-products, if $\chi \in H^1(X_m, \mathbf{Z}/q'\mathbf{Z})$, then $2(\chi \cup \chi) = 0$, and hence $\chi \cup \chi (\text{mod } 2) = 0$. This implies that the cup-product given in the bottom row of this diagram is alternating. By proposition 1.1, we can decompose V_m into a sum of $m/2$ free $\mathbf{F}_p[G]$-modules of rank 2, each of which possessing a non-degenerate hyperbolic form, and such that these $m/2$ spaces are pairwise perpendicular.◇

Proposition 4.2. *Let (X, ϕ) be a $\mathbf{Z}_p$-tower in the Demuškin group X which is not the basic tower; let $q \neq 2$ be the torsion invariant of this tower; and let $\alpha: \mathbf{Z}_p \rightarrow \mathbf{Z}/q\mathbf{Z}^\times$ be the character giving the action of the quotient $X/(\ker(\phi)) \cong \mathbf{Z}_p$ on $I_X^{\ker(\phi)}$. If (X, ψ) is another $\mathbf{Z}_p$-tower in X with the same invariants q and α, then there is an automorphism β of X such that $\psi \circ \beta = \phi$.*

PROOF Let $\aleph = p^m\mathbf{Z}_p$ and $X_m = X_\aleph = \phi^{-1}(\aleph)$. The $\mathbf{Z}/p\mathbf{Z}$-dual of the surjection $X_m \rightarrow \aleph$ is the injection (inflation) $H^1(\aleph, \mathbf{Z}/p\mathbf{Z}) \rightarrow H^1(X_m, \mathbf{Z}/p\mathbf{Z})$, and the image of this map is the subspace generated by ϕ_m. It follows that, as symplectic spaces,

$$V_m \cong \frac{H^1(\aleph, \mathbf{Z}/p\mathbf{Z})^\perp}{H^1(\aleph, \mathbf{Z}/p\mathbf{Z})}.$$

By lemma 4.6, this space possesses a hyperbolic decomposition, and hence the second axiom for a Demuškin formation is satisfied. Since (X,ϕ) is thus a Demuškin formation over $\mathbb{Z}_p$ with invariants n, q, and α, the uniqueness up to an automorphism of X follows from proposition 4.1.◊

§ 4.4 We now turn to $\mathbb{Z}_2$-towers in Demuškin groups, where the torsion-invariant of the tower is 2. We are not able to give a complete classification of such towers, but we do give some necessary invariants which must be considered in any such classification (and in any appropriate definition of the corresponding Demuškin formation).

Thus, let X be a Demuškin 2-group, let $\phi: X \to \mathbb{Z}_2$ be a continuous surjection with kernel V, suppose that I_X^V has order 2. Denote by X' the "cyclotomic subgroup" of X of index 2, and let $V' = X' \cap V$. Then $V/V' = \Delta \cong \mathbb{Z}/2\mathbb{Z}$, $X'/V' = \Gamma \cong \mathbb{Z}_2$, and $X/V' = \Gamma \oplus \Delta$; let δ be the generator of Δ, and let γ be a topological generator for Γ.

If $(X', \text{res}(\phi))$ is not the basic tower of X', then there is a $q = 2^s \geq 4$ so that $I_X^{V'} \cong \mathbb{Z}/q\mathbb{Z}$ as Abelian groups, and we may define the homomorphism

$$\alpha: X/V' \longrightarrow \mathbb{Z}/q\mathbb{Z}^\times$$

which gives the action of X/V' on $I_X^{V'}$. Note that α is determined by the images of γ and of δ. For an appropriate choice of generator γ, we may assume the image of γ is $1 + q'$, where $q' \geq 4$ is the cardinality of $I_X^{X'}$. Being of order 2, $\alpha(\delta)$ can be either -1 or $-1 + 2^{s-1}$ (the third possibility $1 + 2^{s-1}$ is ruled out: it would imply that ${}_4I_X$ was fixed by X, contrary to assumption).

Let $\mathcal{N}_0 = \ker(\alpha)$, and let $X_{\mathcal{N}_0} = \phi^{-1}(\mathcal{N}_0)$. A close inspection of the proof of lemma 4.1 shows that any continuous automorphism υ of X will preserve not only $X_{\mathcal{N}_0}$ and hence q, but also the lattice structure of those subgroups of X which contain $X_{\mathcal{N}_0}$. It follows that under the action of υ, the images $\alpha(\Gamma)$ and $\alpha(\Delta)$ in $\mathbb{Z}/q\mathbb{Z}^\times$ will remain unchanged. In the spirit of proposition 4.2, we thus propose q and $\alpha: \Gamma \oplus \Delta \to \mathbb{Z}/q\mathbb{Z}^\times$ as invariants of the tower (X, ϕ).

Define $\phi_m \in H^1(X_m, \mathbb{Z}/2\mathbb{Z})$ as in § 4.3, and let $\theta_0 \in H^1(X, \mathbb{Z}/2\mathbb{Z})$ be the homomorphism whose kernel is the cyclotomic subgroup X'.

Lemma 4.7. *The homomorphism $\psi \in H^1(X, \mathbb{Z}/2\mathbb{Z})$ lifts to an element $\tilde{\psi} \in$ Hom(X, $\mathbb{Z}_2$) if and only if $\psi \cup \theta_0 = 0$. (We say that ψ lifts to $\tilde{\psi}$ if $\psi = \tilde{\psi}$ (mod 2)).*

PROOF ϕ lifts to such a $\tilde{\phi}$ if and only if ϕ is in the image of $H^1(X, \mathbb{Z}/4\mathbb{Z}) \to H^1(X, \mathbb{Z}/2\mathbb{Z})$, hence if and only if $\phi \in \ker(B)$, where B is the Bockstein operator of § 3.3. By proposition 3.6, we can represent the Bockstein operator by t_0.◇

Let X be a pro-p group, and let q be a power of p. Define the lower q-central series $\{X^{(i,q)}\}$ by letting $X^{(0,q)} = X$ and for $i \geq 1$,

$$X^{(i+1,q)} = X^{(i,q)q}[X, X^{(i,q)}]. \tag{4}$$

Suppose that X is minimally generated by the elements $\{x_1, \ldots, x_n\}$, and let F be the free pro-p group on the generators $\{s_1, \ldots, s_n\}$, with the map $\pi: s_i \mapsto x_i$ defining a presentation of X:

$$1 \longrightarrow R \longrightarrow F \xrightarrow{\pi} X \longrightarrow 1. \tag{4.5}$$

Suppose that $\{\rho_1, \ldots, \rho_r\}$ minimally generate R as a normal subgroup of F. If q is the maximal power of p so that $H^1(F, \mathbb{Z}/q\mathbb{Z}) \cong H^1(X, \mathbb{Z}/q\mathbb{Z})$, then the "transgression" map $tr: H^1(R, \mathbb{Z}/q\mathbb{Z})^X \to H^2(X, \mathbb{Z}/q\mathbb{Z})$ (coming from the Hochschield–Serre spectral sequence associated to (4.4)) is an isomorphism. This allows one to define, for each $\rho \in R$, a map $\varphi_i: H^2(X, \mathbb{Z}/q\mathbb{Z}) \to \mathbb{Z}/q\mathbb{Z}$,

$$\varphi_\rho(f) = tr^{-1}(f)(\rho).$$

Let $\{\chi_1, \ldots, \chi_n\}$ be the dual basis to the images $\{\bar{x}_i\}$ of the generators $\{x_i\}$ in $X/X^{(1,q)}$.

Lemma 4.8. *(Serre) Using the Hall collection process, write $\rho \in R$ in the form,*

$$\rho = \prod_{1 \leq i \leq n} s_i^{a_i q} \prod_{i \leq j} [s_i, s_j]^{a_{i,j}} \rho',$$

with the a_i's and the $a_{i,j}$'s uniquely determined (mod q), and with $\rho' \in F^{(2,q)}$. Then

$$\varphi_\rho(\chi_i \cup \chi_j) = \begin{cases} -a_{i,j}, & \text{if } i \leq j, \\ -(\binom{q}{2})a_i, & \text{if } i = j; \end{cases}$$

and

$$\varphi_\rho(B(\chi_i)) = -a_i,$$

where B is the Bockstein operator.

PROOF See [Ko 2], Sats 7.23 and Sats 7.24.

Corollary. *With the notation of lemma 4.7, cupping with θ_0 represents the homomorphism $\chi \mapsto \chi \cup \chi$.*

PROOF Taking ρ to be a defining relator for the Demuškin group X, it follows from Serre's lemma that $\chi \cup \chi = B(\chi) = \chi \cup \theta_0$.◇

Let $\eta \in H^1(X, \mathbb{Z}/2\mathbb{Z})$ be chosen so that $\phi_0 \cup \eta = 1$. We may further assume that $\eta \cup \theta_0 = 0$: if $\eta \cup \theta_0 = 1$, choose ν so that $\nu \cup (\phi_0 + \theta_0) = 1$—by assumption, $\phi_0 \neq \theta_0$, so this can be done by the non-degeneracy of the cup-product. If $\nu \cup \phi_0 = 1$, let $\eta' = \nu$, while if $\nu \cup \theta_0 = 1$, let $\eta' = \eta + \nu$. Note that $\eta \neq \phi_0$, since $\phi_0 \cup \theta_0 = 0$.

As in § 4.3, define at each level the subspace $V_m = \langle \phi_m, \eta \rangle^{\perp}$. It follows that V_m is for each m a complete subspace of $H^1(X_m, \mathbb{Z}/2\mathbb{Z})$, that the restriction of $\mathrm{res}: H^1(X, \mathbb{Z}/2\mathbb{Z}) \to H^1(X_m, \mathbb{Z}/2\mathbb{Z})$ to V_0 is injective into V_m, and that (following the same proof as for lemma 4.4) cor restricts to a surjection of V_m onto V_0.

Lemma 4.9. *The restriction of the cup-product to V_m is a symmetric, non-degenerate, $G_m = X/X_m$-invariant trace-form, and is non-alternating.*

PROOF At each level m, the cyclotomic subgroup X'_m is the kernel of the homomorphism $\theta_0 = \mathrm{res}(\theta_0) \in V_m$. By the corollary above, if $\chi \in H^1(X_m, \mathbb{Z}/2\mathbb{Z})$, then

$$\begin{aligned} \chi \cup \chi &= \chi \cup \theta_0 \\ &= \mathrm{cor}\chi \cup \theta_0 \\ &= \mathrm{cor}\chi \cup \mathrm{cor}\chi \\ &= \mathrm{res} \circ \mathrm{cor}\chi \cup \chi \\ &= Sp_{G_m}\chi \cup \chi. \end{aligned}$$

Thus the cup-product is a trace-form, and it is non-alternating on V_m since it is non-alternating on V_0: if $\overline{\chi} \cup \overline{\chi} = 1$ in V_0, and $\mathrm{cor}\chi = \overline{\chi}$, then the above computation shows that $\chi \cup \chi = 1$ in V_m.◇

Lemma 4.10. *Let $\mathrm{cor} = \mathrm{cor}_{m,2}: H^1(X_m, \mathbb{Z}/2\mathbb{Z}) \to H^1(X_2, \mathbb{Z}/2\mathbb{Z})$, and given any $g \in G_m$, let $\overline{g}$ be its image in G_2 under the canonical surjection $X/X_m \to X/X_2$. Then for any $\chi \in H^1(X_m, \mathbb{Z}/2\mathbb{Z})$,* $\mathrm{cor}(g.\chi) = \overline{g}.\mathrm{cor}(\chi)$.

PROOF It suffices to prove the lemma with $g = \sigma$, where σ is a generator of G_m. Let s be a lifting to X of σ. Then σ^4 is a generator of X_2/X_m, s^4 is a representative of σ^4 in X_2, and for any $y \in X_2$,

$$\begin{aligned}\operatorname{cor}(\sigma\chi)(y) &= \sigma\chi(\operatorname{Ver}_{X_2 \to X_m} y)\\ &= \chi(s^{-1}(\prod_{0 \leq i \leq 2^{m-2}-1} \widetilde{ys^{4i}}^{-1} ys^{4i})s)\\ &= \chi(\prod \widetilde{ys^{4i}}^{-1} s^{-1}yss^{4i})\\ &= \chi(\prod s^{-1}\widetilde{yss^{4i}}^{-1} s^{-1}yss^{4i})\\ &= \chi(\operatorname{Ver}_{X_2 \to X_m}(s^{-1}ys))\\ &= \bar{\sigma}\chi(y).\diamond\end{aligned}$$

Lemma 4.11. *The Koch-invariant ι_m of the space V_m is dependent only on the tower (X, ϕ).*

PROOF Let $m \geq 2$, and let $\chi \in V_m$ be such that $Sp_{G_m}\chi = \theta_0$. Then $\iota_m = \chi \cup \pi^{2^m-3}$. As in lemma 2.3, we have $\pi^{2^m-3} = \pi\pi^{4(2^{m-2}-1)}$, and $\pi^{4(2^{m-2}-1)} = \operatorname{res} \circ \operatorname{cor}: V_m \to V_2 \to V_m$. Thus

$$\begin{aligned}\iota_m &= \chi \cup \pi^{4(2^{m-2}-1)}\pi\chi\\ &= \operatorname{cor}\chi \cup \bar{\pi}\operatorname{cor}\chi,\end{aligned}$$

Since $Sp_{G_2}\operatorname{cor}\chi = \theta_0$ in V_2, the lemma follows.$\diamond$

Any automorphism of X acts in the obvious way on cochains and induces an action on the cohomology groups $H^i(X, \mathbb{Z}/2\mathbb{Z})$; using proposition 3.1, one can see that the cup-product is invariant under this action. Thus any tower which is the image of ϕ under some automorphism of X will have the same Koch invariant ι_ϕ.

Let (X, ϕ) be a Demuškin tower with tower invariant 2, let X' be the cyclotomic subgroup of X, and let $\Delta = X/X'$. One may thus consider $\operatorname{Hom}(X', \mathbb{Z}_2)$ as a $\mathbb{Z}_2[\Delta]$-module, with the action of Δ on $\psi \in \operatorname{Hom}(X', \mathbb{Z}_2)$ given by: $\delta\psi(x) = \psi(d^{-1}xd)$, where d is any lifting of $\delta \in \Delta$ to X. The restriction map

$$\operatorname{res}: \operatorname{Hom}(X, \mathbb{Z}_2) \to \operatorname{Hom}(X', \mathbb{Z}_2)$$

has image in the subset of homomorphisms fixed by Δ, and whether or not the image of ϕ is a Δ-norm will be left invariant under the action of automorphisms of X (since X' is characteristic in X, any automorphism of X will act on $\mathrm{Hom}(X', \mathbb{Z}_2)$). Let $j_\phi = 0$ if $\mathrm{res}(\phi)$ is a norm, and $j_\phi = 1$ if $\mathrm{res}(\phi)$ is a non-norm.

The author feels that the invariants q, α, ι_ϕ, and j_ϕ are sufficient to distinguish isomorphism classes of towers having tower invariant 2, but suspects them to be interrelated in some way.

§ 4.5. Examples. Let $[x, y]$ be the commutator $x^{-1}y^{-1}xy$, and let x^y denote the conjugation $y^{-1}xy$. If X is a profinite group, and Y is a normal subgroup of finite index in X, let $\mathcal{T}$ be a complete set of left coset representatives; given any $x \in X$, let $\tilde{x} \in \mathcal{T}$ be the corresponding coset representative: $\tilde{x}^{-1}x \in Y$.

Let X be a Demuškin 2-group minimally generated by the n generators $x_1, \ldots, x_n$, let F be a free pro-2 group on the generators $s_1, \ldots, s_n$, and let $\pi\colon F \to X$ be the homomorphism defined by mapping $s_i \mapsto x_i$. The kernel of π is generated as a normal subgroup of F by a single relator ρ, and suitable generators ~~x_i~~and s_i can be found so that ρ has one of the forms given in section 3.4. If Y is a normal subgroup of X with finite quotient G, and if $F' = \pi^{-1}(Y)$, then one has the commutative diagram (with exact rows and columns),

$$\begin{tikzcd}
 & & G \arrow[r, equal] & G & \\
1 \arrow[r] & R \arrow[r] & F \arrow[r, "\pi"] \arrow[u] & X \arrow[r] \arrow[u] & 1 \\
1 \arrow[r] & R \arrow[r] \arrow[u, equal] & F' \arrow[r, "\pi"] \arrow[u] & Y \arrow[r] \arrow[u] & 1.
\end{tikzcd} \tag{4.6}$$

Let $\mathcal{T}$ be a "Schreier transversal" for F' in F: $\mathcal{T}$ is a set of coset representatives t of F' in F such that t can be written as a finite reduced word in the form,

$$t = \prod_{j=1}^{r} s_{i_j}^{\epsilon_j}, \quad \epsilon_j = \pm 1,$$

and such that all "initial segments" $s_{i_1}^{\epsilon_1}, s_{i_1}^{\epsilon_1}s_{i_2}^{\epsilon_2}, \ldots,$ are also in $\mathcal{T}$.

It is a theorem of Schreier (see [S 4], § 3.4) that F' is freely generated by the non-trivial elements

$$\{\widetilde{s_i t}^{-1} s_i t \colon t \in \mathcal{T},\ 1 \le i \le n\}, \tag{4.7}$$

and R is minimally generated as a normal subgroup of F' by the elements (the "Reidemeister–Schreier method"; see [LS 1])

$$\rho_t = t^{-1}\rho t.$$

As will be seen in the example below, if the order of G is 2^m, we will be able to delete $2^m - 1$ of the generators of F' and $2^m - 1$ of the relators ρ_i, leaving one with a minimal presentation of the Demuškin group Y. The main interest in doing all this (and the computations are sometimes rather messy) is that the resulting presentation carries with it the action of G on Y^{ab}. To simplify the notation, we will write the relators ρ_i as relations in X or Y.

Let X be the Demuškin group generated by the elements $\{x_1, \ldots, x_4\}$, with the defining relation

$$1 = x_1^2[x_1, x_2]x_3^4[x_3, x_4], \tag{4.8}$$

and let $\{\chi_i\}$ be the basis of $H^1(X, \mathbb{Z}/2\mathbb{Z})$ which is dual to the basis of $X/X^2[X,X]$ given by the images of the $\{x_i\}$. The cyclotomic subgroup X' of X is (from § 3.4, example (3)) the kernel of χ_2; hence a transversal is $T = \{1, x_2\}$. The generators of X', as computed in (4.7) above, are

$$\{x_1, x_1^{x_2}, x_2^2, x_3, x_3^{x_2}, x_4, x_4^{x_2}\},$$

and we obtain the two relations,

$$1 = x_1^2[x_1, x_2]x_3^4[x_3, x_4] = x_1 x_1^{x_2} x_3^4[x_3, x_4], \tag{4.9}$$

$$1 = x_1^{x_2} x_1^{x_2^2} x_3^{x_2 4}[x_3^{x_2}, x_4^{x_2}] = x_1^{x_2} x_1 [x_1, x_2^2] x_3^{x_2 4}[x_3^{x_2}, x_4^{x_2}]. \tag{4.10}$$

Using (4.10) to write $x_1^{x_2}$ in terms of the other generators, and substituting into (4.9), we find that X' can be generated by the elements

$$S = \{x_1, x_2^2, x_3, x_3^{x_2}, x_4, x_4^{x_2}\},$$

with the defining relation,

$$1 = x_1[x_3^{x_2}, x_4^{x_2}]^{-1}(x_3^{x_2})^{-4}[x_1, x_2^2]^{-1}x_1^{-1}x_3^4[x_3, x_4]. \tag{4.11}$$

Given $x \in X'$, let $\bar{x}$ be the image of x in X'^{ab}. Then X'^{ab} is minimally generated as a $\mathbb{Z}_2$-module by the elements $\{\bar{x}_1, \bar{x}_2^2, \bar{x}_3, \bar{x}_3^{x_2}, \bar{x}_4, \bar{x}_4^{x_2}\}$; the torsion submodule of X'^{ab} is generated by the element $\varsigma = \bar{x}_3^{x_2-1}x_3$; and the action of $\Delta = \{1, \delta\} = X/X'$ on X'^{ab} is given by,

$$\delta.\bar{x}_2^2 = \delta^{-1}.\bar{x}_2^2 = \overline{x_2^{-1}x_2^2x_2} = \bar{x}_2^2, \quad \delta.\bar{x}_3 = \overline{x_2^{-1}x_3x_2} = \bar{x}_3^{x_2} = \varsigma\bar{x}_3,$$

$$\delta.\varsigma = \overline{x_2^{-1}(x_3^{e_3})^{-1}x_3x_2} = \overline{x_3^{-1}x_3^{e_3}} = \varsigma^{-1},$$

and from (4.10),

$$\delta\bar{x}_1 = \bar{x}_1^{-1}\bar{x}_3^{e_3-4}.$$

We may take as free generators of Hom(X′, $\mathbb{Z}_2$) the elements $\{\psi_1, \psi_2, \psi_3, \psi_4, \psi_4'\}$, defined for $s \in S$ by,

$$\psi(s) = \begin{cases} 1, & \text{if } s = x_1, \\ 0, & \text{otherwise.} \end{cases} \quad \psi_2(s) = \begin{cases} 1, & \text{if } s = x_2^2, \\ 0, & \text{otherwise.} \end{cases}$$

$$\psi_4(s) = \begin{cases} 1, & \text{if } s = x_4, \\ 0, & \text{otherwise.} \end{cases} \quad \psi_4'(s) = \begin{cases} 1, & \text{if } s = x_4^{e_4}, \\ 0, & \text{otherwise.} \end{cases}$$

$$\psi_3(s) = \begin{cases} 1, & \text{if } s = x_3, \\ 1, & \text{if } s = x_3^{e_3}, \\ 0, & \text{otherwise.} \end{cases}$$

The Δ-action on these homomorphisms is easily determined; for instance,

$$(\delta.\psi_3)(s) = \psi_3(x_2^{-1}sx_2) = \begin{cases} 1, & \text{if } s = x_3, \\ -4, & \text{if } s = x_1, \\ 0, & \text{otherwise.} \end{cases}$$

Thus we get the actions

$$\delta.\psi_3 = \psi_3 - 4\psi_1,$$

$$\delta.\psi_1 = -\psi_1, \quad \delta.\psi_2 = \psi_2, \quad \delta.\psi_4 = \psi_4'.$$

The submodule of Hom(X′, $\mathbb{Z}_2$) fixed by Δ is freely generated by the elements $\{\psi_2, (1+\delta).\psi_4, \psi_3 - 2\psi_1\}$, and the subspace of Δ-norms is freely generated by $\{2\psi_2, (1+\delta).\psi_4, 2\psi_3 - 4\psi_1\}$.

The $\mathbb{Z}_2$-module Hom(X, $\mathbb{Z}_2$) is freely generated by the homomorphisms $\{\phi_2, \phi_3, \phi_4\}$ defined by

$$\phi_2(x_i) = \begin{cases} 1, & \text{if } i = 2, \\ 0, & \text{otherwise.} \end{cases} \quad \phi_4(x_i) = \begin{cases} 1, & \text{if } i = 4, \\ 0, & \text{otherwise.} \end{cases}$$

$$\phi_3(x_i) = \begin{cases} 1, & \text{if } i = 3, \\ -2, & \text{if } i = 1, \\ 0, & \text{otherwise.} \end{cases}$$

One can now compute the image of res: Hom(X, $\mathbb{Z}_2$) → Hom(X′, $\mathbb{Z}_2$):

$$\text{res}(\phi_2) = 2\psi_2, \quad \text{res}(\phi_3) = \psi_3 - 2\psi_1, \quad \text{res}(\phi_4) = (1+\delta).\psi_4.$$

Using this information, we can thus compute the invariant j_ϕ defined in the previous section, for any explicitly given $\mathbb{Z}_2$-tower (X, ϕ).

Let $\phi = \phi_3 \in \mathrm{Hom}(X, \mathbb{Z}_2)$, and let $X_2 = \phi^{-1}(4\mathbb{Z}_2)$. We now use the above technique to explicitly write down the symplectic structure of the space $H^1(X_2, \mathbb{Z}/2\mathbb{Z})$. In view of lemmas 4.10 and 4.11, this will allow us to compute the Koch invariant ι of the tower (X, ϕ).

We take as our transversal T of X_2 in X the set $\{1, x_3, x_3^2, x_3^3\}$, and use (4.7) to obtain the 13 generators:

$$A = x_3^{-2}x_1, A^{x_3}, A^{x_3^2}, A^{x_3^3};\;\; B = x_2, B^{x_3}, B^{x_3^2}, B^{x_3^3};\;\; S = x_3^4;\; C = x_4, C^{x_3}, C^{x_3^2}, C^{x_3^3}.$$

Writing the relation (4.8) in terms of these generators gives

$$1 = A^{x_3^2}(B^{x_3^2})^{-1}ABS(C^{x_3})^{-1}C. \tag{4.12}$$

Conjugating this relation by x_3, x_3^2, and x_3^3 gives the three remaining relations,

$$1 = A^{x_3^3}(B^{x_3^3})^{-1}A^{x_3}B^{x_3}S(C^{x_3^2})^{-1}C^{x_3};$$

$$1 = A[A,S][S,B]b^{-1}A^{x_3^2}B^{x_3^2}S(C^{x_3^3})^{-1}C^{x_3^2};$$

$$1 = A^{x_3}[A^{x_3},S][S,B^{x_3}](B^{x_3})^{-1}A^{x_3^3}B^{x_3^3}S[S,C]c^{-1}C^{x_3^3}.$$

Using these last three relations, we may eliminate the generators $C^{x_3^3}$, $C^{x_3^2}$, and C^{x_3}, and thus obtain the following minimal presentation of X_2: X_2 is minimally generated by the ten elements $\{A, A^{x_3}, A^{x_3^2}, A^{x_3^3}, B, B^{x_3}, B^{x_3^2}, B^{x_3^3}, C, S\}$, subject to a gruesome defining relation of the form,

$$\begin{aligned}1 = {} & A^2(A^{x_3})^2(A^{x_3^2})^2(A^{x_3^3})^2S^4[A,A^{x_3}][A^{x_3},A^{x_3^2}][A^{x_3^2},A^{x_3^3}][A^{x_3^3},A][B,B^{x_3}][B^{x_3},B^{x_3^2}][B^{x_3^2},B^{x_3^3}][B^{x_3^3},B]\\ & [A,B][A,B^{x_3}][A,B^{x_3^2}][A^{x_3},B^{x_3}][A^{x_3},B^{x_3^2}][A^{x_3},B][A^{x_3^2},B^{x_3^2}][A^{x_3^2},B^{x_3^3}][A^{x_3^3},B^{x_3}]\\ & [A^{x_3^3},B^{x_3^3}][A^{x_3^3},B][A^{x_3^3},B^{x_3^2}][A,S][B,S][A^{x_3},S][B^{x_3},S][C,S]\rho',\end{aligned} \tag{4.13}$$

with $\rho' \in X_2^{(2,2)}$.

Let $G = X/X_2$, and let σ be the image of x_3 in G. Then the action of G on X_2^{ab} can be read off the generators, noting that from (4.12) one has

$$C^{x_3} \equiv CABA^{x_3^2}(B^{x_3^2})^{-1}S \mod [X_2, X_2].$$

Let $\{\hat{A}_i, \hat{B}_i, \hat{C}, \hat{S} : i = 0,1,2,3\}$ be the basis of $H^1(X_2, \mathbb{Z}/2\mathbb{Z})$ dual to the basis of $X_2/X_2^2[X_2, X_2]$ given by our generators of X_2. Using the rule $\sigma.f(x) = f(x^{\sigma_2})$ for $f \in H^1(X_2, \mathbb{Z}/2\mathbb{Z})$ and $x \in X_2$, we obtain the following G-module structure of $H^1(X_2, \mathbb{Z}/2\mathbb{Z})$:

$$\sigma\hat{C} = \hat{C}, \quad \sigma\hat{S} = \hat{S} + \hat{C}, \quad \sigma\hat{A}_0 = \hat{A}_3 + \hat{C}, \quad \sigma\hat{A}_3 = \hat{A}_2, \quad \sigma\hat{A}_2 = \hat{A}_1 + \hat{C},$$

$$\sigma\hat{A}_1 = \hat{A}_0, \quad \sigma\hat{B}_0 = \hat{B}_3 + \hat{C}, \quad \sigma\hat{B}_3 = \hat{B}_2, \quad \sigma\hat{B}_2 = \hat{B}_1 + \hat{C}, \quad \sigma\hat{B}_1 = \hat{B}_0.$$

Let $\phi_{(2)} = \frac{1}{2}\mathrm{res}(\phi) \pmod 2$. Then

$$\phi_{(2)} = \hat{A}_0 + \hat{A}_1 + \hat{A}_2 + \hat{A}_3 + \hat{S}.$$

Since in $H^1(X, \mathbb{Z}/2\mathbb{Z})$ one has $\phi_{(0)} \cup \chi_4 = \chi_3 \cup \chi_4 = 1$, it follows from lemma 4.2 that $\mathrm{res}(\chi_4) \cup \phi_{(2)} = 1$. Noting that $\mathrm{res}(\chi_4) = \hat{C}$, we let $V_2 = \langle \phi_{(2)}, \hat{C} \rangle^{\perp}$. One now uses the form of the relation (4.13) and lemma 4.8 to show that V_2 is a free $\mathbb{F}_2[G]$-module generated by $\hat{A}_0$ and $\hat{B}_0$. Now

$$\mathrm{res}(\theta_0) = \hat{B}_0 + \hat{B}_1 + \hat{B}_2 + \hat{B}_3 = Sp_G\hat{B}_0,$$

so that the Koch invariant of V_2, and hence of the tower (X, ϕ), is given by

$$\iota = \hat{B}_0 \cup \pi\hat{B}_0 = \hat{B}_0 \cup (\hat{B}_0 + \hat{B}_3 + \hat{C}) = 1.$$

Bibliography

[Bo 1] N. Bourbaki, *Algebra*, Hermann (1969).

[B 1] A. Brumer, "Pseudocompact Algebras, Profinite Groups, and Class Formations", *J. Algebra* 4,(1966).

[D 1] V. Diekert, 'Über die Absolute Galoisgruppe dyadischer Zahlkörper," *Journal fur die reine und angewandte Mathematik* 350 (1984).

[FM 1] A. Frölich,A. M. McEvett, "Forms Over Rings with Involution," *Jour. Alg.* 12, (1969).

[H 1] K. Haberland, "Galois Cohomology of Algebraic Number Fields," VEB Deutcher Verlag der Wissenschaften, (1978).

[JW 1] U. Jannsen, K. Wingberg, "Die Struktur der absoluten Galoisgruppe p-adischer Zahlkörper," *Invent. Math.* 47, (1982).

[Ja 1] A. V. Jakovlev, "Symplectic Spaces with Operators over Commutative Rings," *Vestnik Leningrad Univ.* 25, (1970).

[Ja 2] A.V. Jakovlev, "The Galois Group of the Algebraic Closure of a Local Field," *Math. USSR–Izvestija* 2, (1968).

[Ja 3] A. V. Jakovlev, "On the Theory of Symplectic Spaces with Operators," *Sibirskii Matematicheskii Zhurnal*, 26, (1975).

[Ja 4] A. V. Jakovlev, "Structure of the Multiplicative Group of a Simply Ramified Extension of a Local Field of Odd Degree," *Math. USSR Sbornik* , 35, (1979).

[K 1] Y.Kawada, "On the Structure of the Galois Group of Some Infinite Extensions II," *J. Fac. Science, U. Tokyo Soc.* I, (1954).

[Ko 1] H. Koch, "Uber Darstellungsräume und die Struktur der multiplikativen Gruppe eines p-adischen Zahlkörpers," *Math. Nachr.* 26, (1963).

[Ko 2] H. Koch, "Galoissche Theorie der p-Erweiterungen," *Springer-Verlag*, (1970).

[Ko 3] H. Koch, "Uber das Normenrestsymbol einer lokalen unverzweigten Erweiterung von 2-Potenzgrad," *Math. Nachr.* 53, (1972).

[Ko 4] H. Koch, "The Galois Group of a p-Closed Extension of a Local Field," *Soviet Math. Dokl.* 19, (1978).

[Kn 1] M. Kneser, "Zum expliziten Resiprositätsgesets von I. R. Šafarevič," *Math. Nachr.* 6, (1951/1952).

[L 1] J. P. Labute, "Classification of Demuškin Groups," *Canadian Journal of Mathematics* 19, (1967).

[La 1] S. Lang, "Algebra," Addison–Wesley (1967).

[LS 1] R. C. Lyndon, P. E. Schupp, "Combinatorial Group Theory," Springer–Verlag, (1977).

[S 1] J. P. Serre, "Corps Locaux," Hermann, (1962).

[S 2] J. P.Serre, "Cohomologie Galoisienne," *Lecture Notes in Mathematics* 7, (1963)

[S 3] J. P.Serre, "Structure de Certains Pro-p Groupes," *Seminaire Bourbaki* 252, (1962).

[S 4] J. P. Serre, "Trees," Springer-Verlag (1980).

[Sh 1] S. Shatz, "Profinite Groups, Arithmetic, and Algebraic Geometry," Princeton University Press, (1972).

[Sha 1] I. R. Shafarevich, "A General Reciprocity Law," *Math. Sborn.* 26, (1950).

[W 1] C. T. C. Wall, "Norms of Units in Group Rings," *Proceedings, London Math. Soc.* 29,(1974).

[Wi 1] K. Wingberg, "Der Eindeutigkeitssatz für Demuškinformationen," *Inven. Math.* 70, (1982).

[Z 1] G. Zelvenskii, "On the Algebraic Closure of a Local Field for $p = 2$," *Math USSR–Isvestija* 6, (1972).