INSTITUTUL DE MATEMATICĂ
AL ACADEMIEI ROMÂNE

PREPRINT SERIES OF THE INSTITUTE OF MATHEMATICS
OF THE ROMANIAN ACADEMY

ISSN 0250 3638

TOWARD AN ABSTRACT COGALOIS THEORY (I): KNESER AND COGALOIS GROUPS OF COCYCLES

by
Toma ALBU and Serban BASARAB

Preprint nr. 1/2003

BUCUREŞTI

TOWARD AN ABSTRACT COGALOIS THEORY (I): KNESER AND COGALOIS GROUPS OF COCYCLES

by

TOMA ALBU[1] and SERBAN BASRAB[2]

January, 2003

1 Atilim University, Department of Mathematics 06836 Incek, Ankara, TURKEY, albu@atilim.edu.tr, Toma.Albu@imar.ro
2 Institute of Mathematics "Simion Stoilow" of the Romanian Academy, P.O.Box 1–764, RO–70700 Bucharest 1, ROMANIA, Serban.Basarab@imar.ro

TOWARD AN ABSTRACT COGALOIS THEORY (I): KNESER AND COGALOIS GROUPS OF COCYCLES

TOMA ALBU
Atilim University, Department of Mathematics
06836 Incek, Ankara, TURKEY
and
Institute of Mathematics "Simion Stoilow" of the Romanian Academy
P.O. Box 1–764
RO – 70700 Bucharest 1, ROMANIA
e-mail: `albu@atilim.edu.tr`, `Toma.Albu@imar.ro`

ŞERBAN BASARAB *
Institute of Mathematics "Simion Stoilow" of the Romanian Academy
P.O. Box 1–764
RO – 70700 Bucharest 1, ROMANIA
e-mail: `Serban.Basarab@imar.ro`

December 28, 2002

Abstract

This is the first part of a series of papers which aim to develop an abstract group theoretic framework for the Cogalois Theory of field extensions.

2000 *Mathematics Subject Classification*: 20E18, 12G05, 12F10, 12F99.

Key words and phrases: Profinite group, Abelian torsion group, continuous 1-cocycle, Abstract Galois Theory, Abstract Kummer Theory, Abstract Cogalois Theory, Kneser group of cocycles, Cogalois group of cocycles.

*The second author gratefully acknowledges partial support from the Grant 47/2002 awarded by the Romanian Academy.

Introduction

The efforts to generalize the famous *Gauss' Quadratic Reciprocity Law* led to the theory of Abelian extensions of algebraic and p-adic number fields, known as *Class Field Theory*. This theory can be also developed in an abstract group theoretic framework, namely for arbitrary profinite groups. Since the profinite groups are precisely those topological groups which arise as Galois groups of Galois extensions, an *Abstract Galois Theory* for arbitrary profinite groups was developed within the *Abstract Class Field Theory* (see e.g., Neukirch [11]).

The aim of this paper is to present a dual theory we called *Abstract Cogalois Theory* to the *Abstract Galois Theory*. Roughly speaking, *Cogalois Theory* (see Albu [2]) investigates field extensions, finite or not, which possess a Cogalois correspondence. This theory is somewhat dual to the very classical *Galois Theory* dealing with field extensions possessing a Galois correspondence.

The basic concepts of Cogalois Theory, namely that of *G-Kneser* and *G-Cogalois* field extension, as well as their main properties are generalized to arbitrary profinite groups. More precisely, let Γ be an arbitrary profinite group, and let A be any subgroup of the Abelian group $\mathbb{Q}/\mathbb{Z}$ such that Γ acts continuously on the discrete group A. Then, one defines the concepts of *Kneser* subgroup and *Cogalois* subgroup of the group $Z^1(\Gamma, A)$ of all continuous 1-cocycles of Γ with coefficients in A, and one establish their main properties. Thus, we prove an *Abstract Kneser Criterion* for Kneser groups of cocycles, as well as a *Quasi-Purity Criterion* for Cogalois groups of cocycles.

The idea to involve the group $Z^1(\Gamma, A)$ in defining the abstract concepts mentioned above comes from the description, via the Hilbert's Theorem 90, of the Cogalois group $\mathrm{Cog}(E/F)$ of an arbitrary Galois extension E/F as a group canonically isomorphic to the group $Z^1(\mathrm{Gal}(E/F), \mu(E))$ of all continues 1-cocycles of the profinite Galois group $\mathrm{Gal}(E/F)$ of the extension E/F with coefficients in the group $\mu(E)$ of all roots of unity in E. Note that the multiplicative group $\mu(E)$ is isomorphic (in a noncanonical way) to a subgroup of the additive group $\mathbb{Q}/\mathbb{Z}$, and that the basic groups appearing in the investigation of E/F from the Cogalois Theory perspective are subgroups of $\mathrm{Cog}(E/F)$. In this way, the above description of $\mathrm{Cog}(E/F)$ in terms of 1-cocycles naturally suggests to study the abstract setting of subgroups of groups of type $Z^1(\Gamma, A)$, with Γ an arbitrary profinite group and A any subgroup of $\mathbb{Q}/\mathbb{Z}$ such that Γ acts continuously on the discrete group A.

In the forthcoming Part II of this paper we introduce the concept of *Cogalois action*, and provide a complete description of the category of all these actions.

In Part III we apply our general theory to retrieve the abstract Kummer Theory, and we show how some basic results as well as some new results of the field theoretic Cogalois Theory can be easily obtained from our abstract approach.

0 Notation and Terminology

Throughout this paper Γ will denote a fixed profinite group with identity element denoted by 1, and A will always be a fixed subgroup of the Abelian group $\mathbb{Q}/\mathbb{Z}$ such that Γ acts continuously on A endowed with the discrete topology, i.e., A is a discrete Γ-module.

We denote by $\mathbb{N}$ the set $\{1, 2, \ldots\}$ of all positive natural numbers, by $\mathbb{P}$ the set of positive prime numbers, by $\mathbb{Z}$ the ring of all rational integers, by $\mathbb{Q}$ the field of all rational numbers, by $\mathbb{R}$ the field of all real numbers, and by $\mathbb{C}$ the field of all complex numbers. For any integers $k,\, m \in \mathbb{Z}$ we shall denote by $k \bmod m$ the congruence class $k + m\mathbb{Z}$ of k modulo m; if $n \in \mathbb{N}$ is a divisor of of m, then we shall write occasionally $k + m\mathbb{Z} \bmod n$ instead of $k \bmod n$. For any ring R with identity element, R^* will denote the group of units of R. If q is a power of a prime number, then we denote by $\mathbb{F}_q$ the finite field with q elements.

For any $n \in \mathbb{N}$, $n \geqslant 2$ we denote by $\mathbb{D}_{2n}$ the dihedral group of order $2n$. The group of quaternions will be denoted by Q. Given an action of a group C on a group D, the semidirect product of C by D is denoted by $D \rtimes C$, with a suitable subscript, if necessary, to specify the action.

For any $p \in \mathbb{P}$ we denote by $\mathbb{Z}_p$ the ring of p-adic integers, by $\mathbb{Q}_p$ the field of p-adic numbers, and by $\mathbb{Z}_{p^\infty}$ the quasi-cyclic group of type p^∞, that is, the p-primary component $(\mathbb{Q}/\mathbb{Z})(p)$ of the quotient group $\mathbb{Q}/\mathbb{Z}$. Note that $\mathbb{Z}_{p^\infty} \cong \mathbb{Q}_p/\mathbb{Z}_p$.

For any $r \in \mathbb{Q}$, the coset of r in the quotient group $\mathbb{Q}/\mathbb{Z}$ will be denoted by $\widehat{r}$. The elements of Γ will be denoted by small Greek letters σ, τ, ρ, and the elements of A by a, b, c. The action of $\sigma \in \Gamma$ on $a \in A$ will be denoted by σa. The set of all elements of A invariant under the action of Γ will be denoted as usually by A^Γ.

An Abelian group C is said to be of *of bounded order* if $kC = \{0\}$ for some $k \in \mathbb{N}$; if C is of bounded order, then the *exponent* $\exp(C)$ of C is the least $n \in \mathbb{N}$ such that $nC = \{0\}$. The order of an element $x \in C$ will be denoted $\mathrm{ord}(x)$. If n is a positive integer, and D is an Abelian torsion group, then we shall use the notation $D[n] := \{\, x \in D \mid nx = 0 \,\}$. For any $p \in \mathbb{P}$ we denote by $D(p)$ the p-primary component of D. By $\mathcal{O}_D$ we denote the set of all $n \in \mathbb{N}$ for which there exists $x \in D$ of order n, i.e., $D[n]$ has exponent n. With respect to the divisibility relation and the operations gcd and lcm, $\mathcal{O}_D$ is a distributive lattice with the least element 1. $\mathcal{O}_D$ has a last element if and only if D is a group of bounded order, and in this case, the last element of $\mathcal{O}_D$ is precisely $\exp(D)$.

For any topological group T we denote by $\mathbb{L}(T)$ the lattice of all subgroups of T, and by $\overline{\mathbb{L}}(T)$ the lattice of all closed subgroups of T. The notation $U \leqslant T$ means that U is a subgroup of T. For any $U \leqslant T$ we denote by $\mathbb{L}(T \,|\, U)$ (resp. $\overline{\mathbb{L}}(T \,|\, U)$) the lattice of all subgroups (resp. closed subgroups) of T lying over U. If $X \subseteq T$, then $\overline{X}$ will denote the closure of X, and $\langle X \rangle$ will denote the subgroup generated by X. The notation $U \lhd T$ means that U is a normal subgroup of T. For a subgroup U of T we shall denote by T/U the set $\{\, tU \mid t \in T \,\}$ of all left cosets of U in T. We denote by $\mathrm{Ch}(T)$ or by $\widehat{T}$ the *character group* of T, that is, the group of all continuous homomorphisms of T into the unit circle $\mathbb{U} = \{\, z \mid z \in \mathbb{C},\ |z| = 1 \,\}$. If S is another topological group, then $\mathrm{Hom}(S, T)$ will denote the set of all continuous group morphisms from S to T.

Recall that a *crossed homomorphism* (or an 1-*cocycle*) of Γ with coefficients in A is a map $f : \Gamma \to A$ such that $f(\sigma\tau) = f(\sigma) + \sigma f(\tau)$, $\sigma, \tau \in \Gamma$; in particular, $f(1) = 0$. The set of all continuous crossed homomorphisms of Γ with coefficients in A is an Abelian group, which will be denoted by $Z^1(\Gamma, A)$. Note that, in fact, $Z^1(\Gamma, A)$ is a torsion group. Indeed, since Γ is a profinite group and A is a discrete space, a map $h : \Gamma \longrightarrow A$ is continuous if and only if h is locally constant, that is, there exists an open normal subgroup Δ (in particular, of finite index in Γ) such that h factorizes through the canonical surjection map $\Gamma \to \Gamma/\Delta$. Since A is a torsion group, it follows now that for any continuous map $h : \Gamma \longrightarrow A$ there exists an $n \in \mathbb{N}$ such that $h(\Gamma) \subseteq (1/n)\mathbb{Z}/\mathbb{Z}$, and then $nh = 0$, i.e., h has finite order.

The elements of $Z^1(\Gamma, A)$ will be denoted by f, g, h. Always G, H will denote subgroups of $Z^1(\Gamma, A)$ and Δ, Λ subgroups of Γ. For every $a \in A$ we shall denote by f_a the 1-*coboundary* $f_a : \Gamma \to A$, defined as $f_a(\sigma) = \sigma a - a$, $\sigma \in \Gamma$. The set $B^1(\Gamma, A) := \{ f_a \mid a \in A \}$ is a subgroup of $Z^1(\Gamma, A)$. The quotient group $Z^1(\Gamma, A)/B^1(\Gamma, A)$ is called the first cohomology group of Γ with coefficients in A, and is denoted by $H^1(\Gamma, A)$.

Consider the *evaluation map*

$$\langle -, - \rangle : \Gamma \times Z^1(\Gamma, A) \longrightarrow A, \quad \langle \sigma, h \rangle = h(\sigma).$$

For any $\Delta \leqslant \Gamma$, $G \leqslant Z^1(\Gamma, A)$, $g \in Z^1(\Gamma, A)$, and $\gamma \in \Gamma$ denote

$$\begin{aligned}
\Delta^\perp &= \{ h \in Z^1(\Gamma, A) \mid \langle \sigma, h \rangle = 0, \ \forall \, \sigma \in \Delta \}, \\
G^\perp &= \{ \sigma \in \Gamma \mid \langle \sigma, h \rangle = 0, \ \forall \, h \in G \}, \\
g^\perp &= \{ \sigma \in \Gamma \mid \langle \sigma, g \rangle = 0 \}, \\
\gamma^\perp &= \{ h \in Z^1(\Gamma, A) \mid \langle \gamma, h \rangle = 0 \}.
\end{aligned}$$

One verifies easily that $\Delta^\perp \leqslant Z^1(\Gamma, A)$, $G^\perp \leqslant \Gamma$, and $g^\perp = \langle g \rangle^\perp$. Observe that $g^\perp$ is the set of zeroes of the continuous map g from Γ to the discrete group A, hence it is an open subgroup of Γ. Since $G^\perp = \bigcap_{g \in G} g^\perp$, it follows that $G^\perp \in \overline{\mathbb{L}}(\Gamma)$.

The group $Z^1(\Gamma, A)$ is clearly a discrete left Γ-module with respect to the following action: $(\sigma h)(\tau) = \sigma h(\sigma^{-1}\tau\sigma)$, σ, $\tau \in \Gamma$, $h \in Z^1(\Gamma, A)$. If $\sigma \in \Gamma$ and $G \in \mathbb{L}(Z^1(\Gamma, A))$, then

$$(\sigma G)^\perp = \sigma G^\perp \sigma^{-1}.$$

For any $\Delta \in \mathbb{L}(\Gamma)$ one denotes by

$$\mathrm{res}^\Gamma_\Delta : Z^1(\Gamma, A) \longrightarrow Z^1(\Delta, A), \ h \mapsto h|_\Delta,$$

the restriction map.

The next result collects together the main properties of the assignments $(-)^\perp$.

Proposition 0.1. *The following assertions hold.*

(1) *The maps*

$$\mathbb{L}(Z^1(\Gamma, A)) \longrightarrow \overline{\mathbb{L}}(\Gamma),\ G \mapsto G^\perp,$$
$$\overline{\mathbb{L}}(\Gamma) \longrightarrow \mathbb{L}(Z^1(\Gamma, A)),\ \Delta \mapsto \Delta^\perp,$$

establish a Galois connection between the lattices $\mathbb{L}(Z^1(\Gamma, A))$ *and* $\overline{\mathbb{L}}(\Gamma)$, *i.e., they are order-reversing maps and* $X \leqslant X^{\perp\perp}$ *for any element* X *of* $\mathbb{L}(Z^1(\Gamma, A))$ *or* $\overline{\mathbb{L}}(\Gamma)$.

(2) *For any* $\Delta \in \mathbb{L}(\Gamma)$ *and* $G \in Z^1(\Gamma, A)$ *one has*

$$\Delta^\perp = \overline{\Delta}^\perp = \operatorname{Ker}(\operatorname{res}^\Gamma_\Delta) \quad \textit{and} \quad (\operatorname{res}^\Gamma_\Delta(G))^\perp = G^\perp \cap \Delta.$$

(3) *For any* $G_1,\ G_2 \in Z^1(\Gamma, A)$ *and* $\Delta_1,\ \Delta_2 \in \mathbb{L}(\Gamma)$ *one has*

$$(G_1 + G_2)^\perp = G_1^\perp \cap G_2^\perp \quad \textit{and} \quad \Delta_1^\perp \cap \Delta_2^\perp = \langle \Delta_1 \cup \Delta_2 \rangle^\perp.$$

Proof. The proof is straightforward, and therefore is left to the reader. □

Remarks 0.2. (1) Clearly, we have

$$\begin{aligned} 1^\perp &= Z^1(\Gamma, A), \\ \Gamma^\perp &= \{0\}, \\ 0^\perp &= \Gamma. \end{aligned}$$

Note that $(Z^1(\Gamma, A))^\perp$ is a closed normal subgroup of Γ contained in the closed normal subgroup $(B^1(\Gamma, A))^\perp$, the kernel of the action of Γ on A. Setting $H^1(\Gamma, A)^\perp = B^1(\Gamma, A)^\perp / Z^1(\Gamma, A)^\perp$, we obtain the pairing

$$H^1(\Gamma, A)^\perp \times H^1(\Gamma, A) \longrightarrow A$$

induced by the evaluation map.

(2) Following the standard terminology (see e.g., Stenström [13]), the *closed elements* of the Galois connection given in Proposition 0.1 (1) are the elements X of $\mathbb{L}(Z^1(\Gamma, A))$ or $\overline{\mathbb{L}}(\Gamma)$ such that $X = X^{\perp\perp}$. It would be nice to describe effectively such elements. Partial such descriptions are given in Lemma 1.5 and in Section 3, Part II.

(3) The last part of Proposition 0.1 can be reformulated by saying that the maps $(-)^\perp$ are semilattice anti-morphisms. One can ask when these maps are actually lattice anti-morphisms, i.e., they also satisfy the following conditions:

$$(G_1 \cap G_2)^\perp = \overline{\langle G_1^\perp \cup G_2^\perp \rangle} \quad \text{and} \quad (\Delta_1 \cap \Delta_2)^\perp = \Delta_1^\perp + \Delta_2^\perp$$

for all $G_1,\ G_2 \in Z^1(\Gamma, A)$ and $\Delta_1,\ \Delta_2 \in \mathbb{L}(\Gamma)$.

In Section 2 we will discuss cases when the maps $(-)^\perp$ establish lattice anti-isomorphisms between certain sublattices of $\mathbb{L}(Z^1(\Gamma, A))$ and $\overline{\mathbb{L}}(\Gamma)$, while in Section 4, Part II we will see that for certain actions we called *Cogalois actions* we do obtain lattice anti-isomorphisms between $\mathbb{L}(Z^1(\Gamma, A))$ and $\overline{\mathbb{L}}(\Gamma)$. □

1 Kneser groups of cocycles

In this section we define the concept of abstract Kneser group and establish the abstract version of the field theoretic Kneser Criterion [10].

Lemma 1.1. *If G is a finite subgroup of $Z^1(\Gamma, A)$, then $(\Gamma : G^{\perp}) \leqslant |G|$.*

Proof. First assume that G is a finite cyclic group, and let $h \in Z^1(\Gamma, A)$ be a generator. Then $G^{\perp} = h^{\perp}$. The map $h : \Gamma \longrightarrow A$ induces an injective map $\Gamma/h^{\perp} \longrightarrow A$. Since $h^{\perp}$ is an open subgroup of Γ it follows that the index $(\Gamma : h^{\perp}) = |\, h(\Gamma)\, |$ is finite and bounded above by the order, say n, of the (cyclic) subgroup of A generated by $h(\Gamma)$. As n is the lcm of the orders of $h(\sigma)$ for $\sigma \in \Gamma$, one easily deduces that $n = |G|$, as desired.

Now assume that G is an arbitrary finite subgroup of $Z^1(\Gamma, A)$, and write G as a direct sum $G = \bigoplus\limits_{1 \leqslant i \leqslant k} G_i$ of finitely many cyclic subgroups $G_i = \langle h_i \rangle$, $1 \leqslant i \leqslant k$. Observe that, by the above considerations, $\langle h_i(\Gamma) \rangle$ is a cyclic group of order $|G_i|$, and hence $\langle h_i(\Gamma) \rangle \cong \langle h_i \rangle$ for every $i = 1, \ldots k$. As $G^{\perp} = \bigcap_{1 \leqslant i \leqslant k} G_i^{\perp} = \bigcap_{1 \leqslant i \leqslant k} h_i^{\perp}$, we obtain an embedding of the quotient set $\Gamma/G^{\perp}$ into $\prod_{1 \leqslant i \leqslant k} \Gamma/G_i^{\perp}$. Composing this with the canonical embedding

$$\prod_{1 \leqslant i \leqslant k} \Gamma/G_i^{\perp} \longrightarrow \prod_{1 \leqslant i \leqslant k} \langle h_i(\Gamma) \rangle \cong \bigoplus_{1 \leqslant i \leqslant k} G_i = G,$$

we deduce that $(\Gamma : G^{\perp}) \leqslant |G|$, as desired. □

Definition 1.2. *A finite subgroup G of $Z^1(\Gamma, A)$ is called a* Kneser group of $Z^1(\Gamma, A)$ *if $(\Gamma : G^{\perp}) = |G|$.* □

We shall denote by $\mathcal{K}_f(\Gamma, A)$ the set of all finite Kneser groups of $Z^1(\Gamma, A)$. Obviously, $\{0\} \in \mathcal{K}_f(\Gamma, A)$. Since we have seen that $Z^1(\Gamma, A)$ is a left Γ-module, it follows that the set $\mathcal{K}_f(\Gamma, A)$, ordered by inclusion, is a Γ-poset.

Lemma 1.3. *If $G \in \mathcal{K}_f(\Gamma, A)$, then $H \in \mathcal{K}_f(\Gamma, A)$ for any $H \leqslant G$; in other words, $\mathcal{K}_f(\Gamma, A)$ is a lower Γ-poset.*

Proof. By Lemma 1.1, we have $|G| = (\Gamma : G^{\perp}) = (\Gamma : H^{\perp})(H^{\perp} : G^{\perp}) \leqslant |H|\ (H^{\perp} : G^{\perp})$, and so, $(G : H) \leqslant (H^{\perp} : G^{\perp})$.

Let $\widetilde{G} = \{\, g|_{H^{\perp}} \mid g \in G\,\} \leqslant Z^1(H^{\perp}, A)$ be the image of G through the restriction map $\mathrm{res}^{\Gamma}_{H^{\perp}} : Z^1(\Gamma, A) \longrightarrow Z^1(H^{\perp}, A)$. Since $H \subseteq G \cap H^{\perp\perp}$ and $\widetilde{G}^{\perp} = G^{\perp}$, it follows by Lemma 1.1 that

$$(H^{\perp} : G^{\perp}) \leqslant |\widetilde{G}| \leqslant (G : H) \leqslant (H^{\perp} : G^{\perp}),$$

and hence $(H^{\perp} : G^{\perp}) = (G : H)$. So, $(\Gamma : H^{\perp}) = |H|$, as desired. □

Definition 1.4. *A* Kneser group of $Z^1(\Gamma, A)$ *is any subgroup G of $Z^1(\Gamma, A)$ such that $H \in \mathcal{K}_f(\Gamma, A)$ for every finite subgroup H of G.* □

Let $\mathcal{K}(\Gamma, A)$ denote the Γ-poset of all Kneser groups of $Z^1(\Gamma, A)$. By definition, $\mathcal{K}(\Gamma, A)$ is a lower Γ-poset, i.e., $H \in \mathcal{K}(\Gamma, A)$ whenever H is a subgroup of some $G \in \mathcal{K}(\Gamma, A)$. Observe that, by Zorn's Lemma, for any $G \in \mathcal{K}(\Gamma, A)$ there exists a maximal element M of $\mathcal{K}(\Gamma, A)$ such that $G \subseteq M$.

Lemma 1.5. *If $G \in \mathcal{K}(\Gamma, A)$, then $H = G \cap H^{\perp\perp}$ for every $H \in \mathbb{L}(G)$. In particular, if $Z^1(\Gamma, A) \in \mathcal{K}(\Gamma, A)$, then the following statements hold.*

(1) *$H = H^{\perp\perp}$ for every $H \in \mathbb{L}(Z^1(\Gamma, A))$, i.e., every $H \in \mathbb{L}(Z^1(\Gamma, A))$ is a closed element of the Galois connection described in Proposition* 0.1 (1).

(2) *The map $\mathbb{L}(Z^1(\Gamma, A)) \longrightarrow \overline{\mathbb{L}}(\Gamma)$, $H \mapsto H^{\perp}$, is injective.*

Proof. The inclusion $H \subseteq G \cap H^{\perp\perp}$ is obvious. To prove the inverse inclusion, given $g \in G \cap H^{\perp\perp}$, we have to show that $g \in H$. Since $g \in H^{\perp\perp}$, it follows that $H^{\perp} = (H^{\perp\perp})^{\perp} \leqslant g^{\perp}$. As $H^{\perp} = \bigcap_{h \in H} h^{\perp}$, by compactness we deduce that there exists a finitely generated subgroup $H' \leqslant H$ such that $H'^{\perp} \leqslant g^{\perp}$. Since $Z^1(\Gamma, A)$ is a torsion group, it follows that H' is a finite group. Let $G' = \langle H' \cup \{g\} \rangle$. Since the finite groups G' and H' are Kneser as subgroups of G, and $G'^{\perp} = H'^{\perp} \cap g^{\perp} = H'^{\perp}$, we deduce that $|G'| = (\Gamma : G'^{\perp}) = (\Gamma : H'^{\perp}) = |H'|$, and hence $G' = H'$ as $H' \leqslant G'$. Consequently, $g \in H' \leqslant H$, as desired.

Now assume that $Z^1(\Gamma, A) \in \mathcal{K}(\Gamma, A)$. Then (1) is clear since $H^{\perp\perp} \leqslant Z^1(\Gamma, A)$ for any $H \in \mathbb{L}(Z^1(\Gamma, A))$, and (2) follows at once from (1). □

Proposition 1.6. *Let $G \in \mathcal{K}(\Gamma, A)$, $\Delta \in \overline{\mathbb{L}}(\Gamma)$, and denote $\widetilde{G} = \mathrm{res}^{\Gamma}_{\Delta}(G)$, $G' = \Delta^{\perp} \cap G$. Then, the following assertions are equivalent.*

(1) $\widetilde{G} \in \mathcal{K}(\Delta, A)$.

(2) *The inclusion map $\Delta \hookrightarrow G'^{\perp}$ induces a continuous surjection $\Delta \longrightarrow G'^{\perp}/G^{\perp}$.*

(3) *The inclusion map $\Delta \hookrightarrow G'^{\perp}$ induces a homeomorphism $\Delta/\widetilde{G}^{\perp} \longrightarrow G^{\perp\perp}/G^{\perp}$.*

(4) $G'^{\perp} = \Delta G^{\perp}$.

Proof. By assumption, $G \in \mathcal{K}(\Gamma, A)$, so $G' \in \mathcal{K}(\Gamma, A)$ since G' is a subgroup of G and $\mathcal{K}(\Gamma, A)$ is a lower poset. Note that $\Delta \leqslant \Delta^{\perp\perp} \leqslant G'^{\perp}$ and $\widetilde{G}^{\perp} = G^{\perp} \cap \Delta$; hence, the canonical map $\Delta/\widetilde{G}^{\perp} \longrightarrow G'^{\perp}/G^{\perp}$ is injective, and so, (2) $\iff$ (3) $\iff$ (4).

Observe that the morphism $\mathrm{res}^{\Gamma}_{\Delta} : Z^1(\Gamma, A) \longrightarrow Z^1(\Delta, A)$ induces an epimorphism $G \longrightarrow \widetilde{G}$ with kernel $\mathrm{Ker}\,(\mathrm{res}^{\Gamma}_{\Delta}) \cap G = \Delta^{\perp} \cap G = G'$, and hence, an isomorphism $G/G' \cong \widetilde{G}$.

First, assume that G is finite. Then

$$|\widetilde{G}| = (G : G') = |G|\,|G'|^{-1} = (\Gamma : G^{\perp})(\Gamma : G'^{\perp})^{-1} = (G'^{\perp} : G^{\perp}).$$

(1) $\Longrightarrow$ (3): If $\widetilde{G} \in \mathcal{K}(\Delta, A)$, then $(\Delta : \widetilde{G}^{\perp}) = |\widetilde{G}| = (G'^{\perp} : G^{\perp})$; so, the canonical injective map $\Delta/\widetilde{G}^{\perp} \longrightarrow G'^{\perp}/G^{\perp}$ is onto.

(3) $\Longrightarrow$ (1): If the canonical map $\Delta/\widetilde{G}^{\perp} \longrightarrow G'^{\perp}/G^{\perp}$ is bijective, then $|\widetilde{G}| = (G'^{\perp} : G^{\perp}) = (\Delta : \widetilde{G}^{\perp})$, i.e., $\widetilde{G} \in \mathcal{K}(\Delta, A)$.

Next, suppose that G is infinite. Denote by $\mathcal{F}$ the directed set with respect to inclusion of all finite subgroups of G, and set $\widetilde{H} = \mathrm{res}_{\Delta}^{\Gamma}(H)$, $H' = H \cap \Delta^{\perp}$ for every $H \in \mathcal{F}$. Consider the projective system over $\mathcal{F}$ consisting of the family of finite sets $(H'^{\perp}/H^{\perp})_{H\in\mathcal{F}}$ and of the canonical maps $f_{H_1,H_2} : H_2'^{\perp}/H_2^{\perp} \longrightarrow H_1'^{\perp}/H_1^{\perp}$, $H_1, H_2 \in \mathcal{F}$, $H_1 \leqslant H_2$, induced by the inclusion maps $H_2^{\perp} \hookrightarrow H_1^{\perp}$ and $H_2'^{\perp} \hookrightarrow H_1'^{\perp}$. Since $G = \sum\limits_{H\in\mathcal{F}} H$ and $G' = \sum\limits_{H\in\mathcal{F}} H'$, it follows that $G^{\perp} = \bigcap\limits_{H\in\mathcal{F}} H^{\perp}$ and $G'^{\perp} = \bigcap\limits_{H\in\mathcal{F}} H'^{\perp}$. Consequently, the compact totally disconnected space $G'^{\perp}/G^{\perp}$ together with the family of canonical continuous maps $f_H : G'^{\perp}/G^{\perp} \to H'^{\perp}/H^{\perp}, H \in \mathcal{F}$, is the projective limit of the projective system above.

We claim that all the connecting maps f_{H_1,H_2} are onto, which will imply that all the maps f_H are onto too. Indeed, let $H_1, H_2 \in \mathcal{F}$ be such that $H_1 \leqslant H_2$. Since $H_1' = H_1 \cap H_2'$, we have $H_1/H_1' = H_1/(H_1 \cap H_2') \cong (H_1 + H_2')/H_2'$. By assumption, $G \in \mathcal{K}(\Gamma, A)$, and hence, by the proof of Lemma 1.3, it follows that

$$|H_1'^{\perp}/H_1^{\perp}| = |H_1/H_1'|,\ |H_2'^{\perp}/H_2^{\perp}| = |H_2/H_2'|,$$

and

$$|(H_1^{\perp} \cap H_2'^{\perp})/H_2^{\perp}| = |(H_1 + H_2')^{\perp}/H_2^{\perp}| = |H_2/(H_1 + H_2')|.$$

The surjectivity of the map f_{H_1,H_2} is now immediate since for every $\sigma \in H_2'^{\perp}$, the cardinality of the fiber $f_{H_1,H_2}^{-1}(\sigma H_1^{\perp})$ equals $|(H_1^{\perp} \cap H_2'^{\perp})/H_2^{\perp}|$. Consequently, the canonical continuous map $\varphi : \Delta \longrightarrow G'^{\perp}/G^{\perp}$ between compact totally disconnected spaces is onto if and only if $\varphi_H = f_H \circ \varphi : \Delta \longrightarrow H'^{\perp}/H^{\perp}$ is onto for all $H \in \mathcal{F}$.

(1) $\Longrightarrow$ (2): If $\widetilde{G} \in \mathcal{K}(\Delta, A)$, then, by the first part of the proof, for every $H \in \mathcal{F}$, the map φ_H is onto since $\widetilde{H} \in \mathcal{K}(\Delta, A)$ as a subgroup of $\widetilde{G}$. Consequently, the map φ is onto too, as desired.

(2) $\Longrightarrow$ (1): If the map φ is onto, it follows that the map φ_H is onto for every $H \in \mathcal{F}$; hence $\widetilde{H} \in \mathcal{K}(\Delta, A)$ by the first part of the proof. Since any finite subgroup of $\widetilde{G}$ is contained in some $\widetilde{H}$ for $H \in \mathcal{F}$, it follows that $\widetilde{G} \in \mathcal{K}(\Delta, A)$, as desired. □

Corollary 1.7. *Let $G \in \mathcal{K}(\Gamma, A)$, and let $\Delta \in \mathbb{L}(\Gamma)$ be such that $G^{\perp} \subseteq \Delta$. Then $\mathrm{res}_{\Delta}^{\Gamma}(G) \in \mathcal{K}(\Delta, A)$ if and only if $(\Delta^{\perp} \cap G)^{\perp} = \Delta$.* □

Proposition 1.8. *Let $G \leqslant Z^1(\Gamma, A)$, $\Delta \in \mathbb{L}(\Gamma)$, $\widetilde{G} = \mathrm{res}_{\Delta}^{\Gamma}(G)$, and $H = \Delta^{\perp} \cap G$. If $\widetilde{G} \in \mathcal{K}(\Delta, A)$ and $H \in \mathcal{K}(\Gamma, A)$, then $G \in \mathcal{K}(\Gamma, A)$.*

Proof. First, assume that G is a finite group. By assumption, we have

$$(G : H) = |\widetilde{G}| = (\Delta : \widetilde{G}^{\perp}) = (\Delta : G^{\perp} \cap \Delta) \quad \text{and} \quad (\Gamma : H^{\perp}) = |H|.$$

Set $\Lambda = \langle \Delta \cup G^{\perp} \rangle$ and $L = \mathrm{res}_{\Lambda}^{\Gamma}(G)$. Then $L^{\perp} = G^{\perp} \cap \Lambda = G^{\perp}$ by Proposition 0.1 (2). It is easily checked that $\mathrm{res}_{\Delta}^{\Lambda}$ induces an isomorphism $L \stackrel{\sim}{\longrightarrow} \widetilde{G}$. Thus,

$$|\widetilde{G}| = (\Delta : G^{\perp} \cap \Delta) \leqslant (\Lambda : G^{\perp}) = (\Lambda : L^{\perp}) \leqslant |L| = |\widetilde{G}|,$$

and hence

$$(\Lambda : G^{\perp}) = (\Delta : G^{\perp} \cap \Delta) = (G : H).$$

Since $\Lambda \subseteq H^{\perp}$, we obtain

$$|G| = |H|\,(G : H) = (\Gamma : H^{\perp})(\Lambda : G^{\perp}) \leqslant (\Gamma : \Lambda)(\Lambda : G^{\perp}) = (\Gamma : G^{\perp}) \leqslant |G|.$$

Consequently, $(\Gamma : G^{\perp}) = |G|$, i.e., $G \in \mathcal{K}(\Lambda, A)$.

If now G is not necessarily finite, in order to prove that $G \in \mathcal{K}(\Gamma, A)$ we have to show that $G_1 \in \mathcal{K}_f(\Gamma, A)$ for any finite subgroup G_1 of G. Since $\mathrm{res}^{\Gamma}_{\Delta}(G_1) \leqslant \mathrm{res}^{\Gamma}_{\Delta}(G)$, $\Delta^{\perp} \cap G_1 \leqslant \Delta^{\perp} \cap G$, and, by hypotheses, $\mathrm{res}^{\Gamma}_{\Delta}(G)$ and H are Kneser groups of $Z^1(\Delta, A)$ and $Z^1(\Gamma, A)$ respectively, it follows that so are also their subgroups $\mathrm{res}^{\Gamma}_{\Delta}(G_1)$ and $\Delta^{\perp} \cap G_1$ respectively. Then $G_1 \in \mathcal{K}_f(\Gamma, A)$ by the first part of the proof. $\square$

The next two results investigate when an internal direct sum of Kneser subgroups of a given $G \leqslant Z^1(\Gamma, A)$ is also Kneser.

Proposition 1.9. *Let $G \leqslant Z^1(\Gamma, A)$, and assume that G is an internal direct sum of a finite family $(G_i)_{1 \leqslant i \leqslant n}$ of finite subgroups. If $\gcd(|G_i|, |G_j|) = 1$ for all $i \neq j$ in $\{1, \dots, n\}$, then*

$$G \in \mathcal{K}_f(\Gamma, A) \Longleftrightarrow G_i \in \mathcal{K}_f(\Gamma, A), \ \forall\, i,\ 1 \leqslant i \leqslant n.$$

Proof. Assume that every G_i is a Kneser group of $Z^1(\Gamma, A)$. Then,

$$|G| = \prod_{1 \leqslant i \leqslant n} |G_i| = \prod_{1 \leqslant i \leqslant n} (\Gamma : G_i^{\perp}).$$

Since $G^{\perp} \leqslant G_i^{\perp}$, it follows that $(\Gamma : G_i^{\perp}) \mid (\Gamma : G^{\perp})$ for all $i = 1, \dots, n$. But $(\Gamma : G_i^{\perp}) = |G_i|$ are mutually relatively prime by hypothesis, hence $\prod_{1 \leqslant i \leqslant n} (\Gamma : G_i^{\perp}) \mid (\Gamma : G^{\perp})$, and so, $|G| \mid (\Gamma : G^{\perp})$. On the other hand, $(\Gamma : G^{\perp}) \leqslant |G|$ by Lemma 1.1, which implies that $|G| = (\Gamma : G^{\perp})$, i.e., G is a Kneser group.

The implication "$\Longrightarrow$" follows at once from Lemma 1.3. $\square$

Remark 1.10. In general, an internal direct sum of two arbitrary nonzero Kneser subgroups of $Z^1(\Gamma, A)$ is not necessarily Kneser, as the following example shows. Let $\Gamma = \mathbb{D}_6 = \langle\, \sigma, \tau \mid \sigma^2 = \tau^3 = (\sigma\tau)^2 = 1 \,\rangle$, and let $A = (1/3)\mathbb{Z}/\mathbb{Z}$ with the action defined by $\sigma a = -a$, $\tau a = a$ for $a \in A$. The map $Z^1(\Gamma, A) \longrightarrow A \times A$, $g \mapsto (g(\sigma), g(\tau))$ is a group isomorphism. Let $g, h \in Z^1(\Gamma, A)$ be defined by $g(\sigma) = 0$, $h(\sigma) = \widehat{1/3}$, $g(\tau) = h(\tau) = \widehat{1/3}$. Then, it is easily verified that $Z^1(\Gamma, A)$ has two independent Kneser subgroups of order 3, namely, $G := \langle g \rangle$ and $H := \langle h \rangle$, whose (internal direct) sum is not Kneser since $|\Gamma| = 6 < 9 = |G \oplus H|$. $\square$

The next result is the *local-global principle* for Kneser groups.

Corollary 1.11. *A subgroup G of $Z^1(\Gamma, A)$ is a Kneser group if and only if any of its p-primary components $G(p)$ is a Kneser group.*

Proof. For the nontrivial implication, assume that $G(p) \in \mathcal{K}(\Gamma, A)$ for every $p \in \mathbb{P}$. By the definition of the concept of Kneser group we have to prove that any finite subgroup of G is Kneser. Let H be a finite subgroup of G. Then $H(p) = G \cap G(p)$, so $H(p)$ is a Kneser group of $Z^1(\Gamma, A)$ for every $p \in \mathbb{P}$. If $\mathbb{I} := \{p \in \mathbb{P} \mid H(p) \neq 0\}$, then $H = \bigoplus_{p \in \mathbb{I}} H(p)$. Now, observe that $\mathbb{I}$ is finite and $\gcd(|H(p)|, |H(q)|) = 1$ for all $p \neq q \in \mathbb{I}$. Hence H is a Kneser group by Proposition 1.9. □

We are now going to present the main result of this section, namely an abstract version of the Kneser Criterion [10] from Field Theory. To do that, we need some basic notation which will be used in the sequel.

Let $\mathcal{N}(\Gamma, A)$ denote the set (possibly empty) $\mathbb{L}(Z^1(\Gamma, A)) \setminus \mathcal{K}(\Gamma, A)$ of all subgroups of $Z^1(\Gamma, A)$ which are not Kneser groups. Clearly, for any $G \in \mathcal{N}(\Gamma, A)$ there exists at least one minimal member H of $\mathcal{N}(\Gamma, A)$ such that $H \subseteq G$. By $\mathcal{N}(\Gamma, A)_{\min}$ we shall denote the set of all minimal members of $\mathcal{N}(\Gamma, A)$. Observe that whenever $G \in \mathcal{N}(\Gamma, A)_{\min}$, then necessarily G is a nontrivial finite group.

If p is an odd prime number and $\widehat{1/p} \in A \setminus A^{\Gamma}$, define the 1-coboundary

$$\varepsilon_p \in B^1(\Gamma, (1/p)\,\mathbb{Z}/\mathbb{Z}) \leqslant B^1(\Gamma, A)$$

by

$$\varepsilon_p(\sigma) = \sigma\,\widehat{1/p} - \widehat{1/p},\ \sigma \in \Gamma.$$

If $\widehat{1/4} \in A \setminus A^{\Gamma}$, define the map

$$\varepsilon_4' : \Gamma \longrightarrow (1/4)\,\mathbb{Z}/\mathbb{Z}$$

by

$$\varepsilon_4'(\sigma) = \begin{cases} \widehat{1/4} & \text{if } \sigma\,\widehat{1/4} = -\,\widehat{1/4} \\ \widehat{0} & \text{if } \sigma\,\widehat{1/4} = \widehat{1/4} \end{cases}$$

It is easily checked that

$$\varepsilon_4' \in Z^1(\Gamma, (1/4)\,\mathbb{Z}/\mathbb{Z}) \leqslant Z^1(\Gamma, A).$$

Observe that ε_4' has order 4 and $\varepsilon_4 := 2\,\varepsilon_4'$ is the generator of the cyclic group

$$B^1(\Gamma, (1/4)\,\mathbb{Z}/\mathbb{Z}) \leqslant \mathrm{Hom}(\Gamma, A[2])$$

of order 2.

Recall that by $\mathbb{P}$ we have denoted the set of all positive prime numbers. In the sequel we shall use the following notation:

$$\begin{aligned} \mathcal{P} &= (\mathbb{P} \setminus \{2\}) \cup \{4\}, \\ \mathcal{P}(\Gamma, A) &= \{p \in \mathcal{P} \mid \widehat{1/p} \in A \setminus A^{\Gamma}\}. \end{aligned}$$

We shall also use the following notation:

$$B_p = B^1(\Gamma, (1/p)\,\mathbb{Z}/\mathbb{Z}) = B^1(\Gamma, A[p]) = \langle \varepsilon_p \rangle \cong \mathbb{Z}/p\mathbb{Z} \quad \text{if} \quad 4 \neq p \in \mathcal{P}(\Gamma, A),$$

$$B_4 = \langle \varepsilon_4' \rangle \cong \mathbb{Z}/4\mathbb{Z} \quad \text{if} \quad 4 \in \mathcal{P}(\Gamma, A).$$

Recall that we have denoted $\mathcal{O}_G := \{\, \mathrm{ord}(g) \,|\, g \in G \,\}$. For any $G \leqslant Z^1(\Gamma, A)$ we shall denote

$$\mu_G = \bigcup_{n \in \mathcal{O}_G} (1/n)\mathbb{Z}/\mathbb{Z}.$$

Observe that, since $\mathcal{O}_G$ is a directed set with respect to the divisibility relation, μ_G is a subgroup of A, and hence a discrete Γ-submodule of A too. One easily checks that μ_G is the subgroup $\sum_{g\in G} g(\Gamma)$ of $\mathbb{Q}/\mathbb{Z}$ generated by $\bigcup_{g\in G} g(\Gamma)$, and hence it is the smallest subgroup B of A for which $G \leqslant Z^1(\Gamma, B)$. Also note that $\mu_G(p) = \mu_{G(p)} = \bigcup_{g\in G(p)} g(\Gamma)$ for all $p \in \mathbb{P}$.

Lemma 1.12. *With the notation above, we have $\mathcal{N}(\Gamma, A)_{\min} = \{\, B_p \,|\, p \in \mathcal{P}(\Gamma, A) \,\}$.*

Proof. If $4 \neq p \in \mathcal{P}(\Gamma, A)$, then $B_p^{\perp} = \varepsilon_p^{\perp} = \{\, \sigma \in \Gamma \,|\, \sigma\widehat{1/p} = \widehat{1/p} \,\}$ is the kernel of the (nontrivial) action of Γ on $A[p] = (1/p)\mathbb{Z}/\mathbb{Z}$, so $\Gamma/B_p^{\perp}$ is identified with a nontrivial subgroup of $(\mathbb{Z}/p\mathbb{Z})^* = \mathbb{F}_p^*$. Thus $(\Gamma : B_p^{\perp}) \,|\, p-1 < p = |B_p|$, and hence $B_p \in \mathcal{N}(\Gamma, A)_{\min}$.

If $4 \in \mathcal{P}(\Gamma, A)$ then $B_4^{\perp} = \varepsilon_4'^{\perp} = \{\, \sigma \in \Gamma \,|\, \sigma\widehat{1/4} = \widehat{1/4} \,\} = \varepsilon_4^{\perp}$ is the kernel of the (nontrivial) action of Γ on $A[4] = (1/4)\mathbb{Z}/\mathbb{Z}$, so $(\Gamma : B_4^{\perp}) = 2 < 4 = |B_4|$, and hence $B_4 \in \mathcal{N}(\Gamma, A)$. Since the unique proper subgroup of B_4, namely $B^1(\Gamma, A[4]) = \langle \varepsilon_4 \rangle \cong \mathbb{Z}/2\mathbb{Z}$, belongs to $\mathcal{K}(\Gamma, A)$ as $(\Gamma : \varepsilon_4^{\perp}) = 2 = \mathrm{ord}(\varepsilon_4)$, it follows that $B_4 \in \mathcal{N}(\Gamma, A)_{\min}$.

Thus, we proved the inclusion $\{\, B_p \,|\, p \in \mathcal{P}(\Gamma, A) \,\} \subseteq \mathcal{N}(\Gamma, A)_{\min}$. To prove the opposite inclusion, let $G \in \mathcal{N}(\Gamma, A)_{\min}$. Then necessarily G is a nontrivial finite group. Decomposing G as the internal direct sum $G = \bigoplus_{p\in\mathbb{I}} G(p)$ of its nonzero p-primary components, and using Corollary 1.11 we deduce that the finite subset $\mathbb{I}$ of $\mathbb{P}$ is a singleton, in other words, G is a p-group for some prime number p. Then $\mu_G = (1/p^n)\mathbb{Z}\,/\mathbb{Z}$ for some $n \geqslant 1$, and there exist $g \in G$ and $\sigma \in \Gamma$ such that $g(\sigma) = \widehat{1/p^n}$.

As we have already noticed, $G \leqslant Z^1(\Gamma, \mu_G)$. Obviously, $G \in \mathcal{N}(\Gamma, \mu_G)_{\min}$, so we may assume from the beginning that $A = \mu_G = (1/p^n)\mathbb{Z}/\mathbb{Z}$. Let $\Delta := B^1(\Gamma, A)^{\perp}$ denote the kernel of the action of Γ on A. We claim that $\Delta \subseteq G^{\perp}$, i.e., $\widetilde{G} := \mathrm{res}^{\Gamma}_{\Delta}(G) = \{0\}$. In particular, this will imply that $n \geqslant 2$ for $p = 2$, for otherwise, if $n = 1$ and $p = 2$ we would have $\Delta = \Gamma = G^{\perp}$, and hence $G \leqslant G^{\perp\perp} = \Gamma^{\perp} = \{0\}$, which is a contradiction.

Assume the contrary, i.e., $\Delta \nsubseteq G^{\perp}$. Then $\Delta^{\perp} \cap G \neq G$, and hence $\Delta^{\perp} \cap G \in \mathcal{K}(\Gamma, A)$ as $G \in \mathcal{N}(\Gamma, A)_{\min}$. By Proposition 1.8, it remains to show that $\widetilde{G} \in \mathcal{K}(\Delta, A)$ to obtain that $G \in \mathcal{K}(\Gamma, A)$, contrary to our assumption.

Note that $\widetilde{G} \leqslant Z^1(\Delta, A) = \mathrm{Hom}(\Delta, A)$, so $\widetilde{G}^{\perp} = G^{\perp} \cap \Delta = \bigcap\limits_{h\in G} \mathrm{Ker}(h|_{\Delta})$ is an open normal subgroup of Δ, $\Delta/\widetilde{G}^{\perp}$ is a finite Abelian group, and $\widetilde{G}$ is embedded into

$$\mathrm{Hom}(\Delta/\widetilde{G}^{\perp},\ A) \leqslant \mathrm{Hom}(\Delta/\widetilde{G}^{\perp},\ \mathbb{Q}/\mathbb{Z}) = \mathrm{Ch}(\Delta/\widetilde{G}^{\perp}) \cong \Delta/\widetilde{G}^{\perp}.$$

Consequently, by Lemma 1.1, $(\Delta : \widetilde{G}^{\perp}) \leqslant |\widetilde{G}| \leqslant (\Delta : \widetilde{G}^{\perp})$, i.e., $\widetilde{G} \in \mathcal{K}(\Delta, A)$, as desired. This proves the claim that $\Delta \leqslant G^{\perp}$.

Thus G can be identified with a subgroup of $Z^1(\Gamma/\Delta, A)$, and moreover $G \in \mathcal{N}(\Gamma/\Delta, A)_{\min}$, so we may assume without loss of generality that Γ is a subgroup of $(\mathbb{Z}/p^n\mathbb{Z})^*$ acting (faithfully) by multiplication on $A := (1/p^n)\mathbb{Z}/\mathbb{Z}$, $G \in \mathcal{N}(\Gamma, A)_{\min}$, and $\mu_G = A$, i.e., $g(\tau) = \widehat{1/p^n}$ for some $g \in G$ and $\tau \in \Gamma$. Recall that $n \geqslant 1$ for $p \neq 2$, and $n \geqslant 2$ for $p = 2$.

First, note that G is cyclic of order p^n, generated by g. Indeed, assuming the contrary, it follows that the proper subgroup G' of G generated by g is a Kneser group of $Z^1(\Gamma, A)$ since $G \in \mathcal{N}(\Gamma, A)_{\min}$, so

$$p^n = |G'| = (\Gamma : G'^{\perp}) \leqslant |\Gamma| \leqslant \varphi(p^n) = p^{n-1}(p-1),$$

which is a contradiction. By the same reason it follows that the subgroup pG, properly contained in G, is a Kneser group of $Z^1(\Gamma, A)$, hence $(\Gamma : (pG)^{\perp}) = |pG| = p^{n-1}$. This implies that $p^{n-1} \,|\, |\Gamma|$ and $|(pG)^{\perp}| = (|\Gamma| : p^{n-1}) \,|\, (\varphi(p^n) : p^{n-1})$, and so, $t := |(pG)^{\perp}|$ is a divisor of $p-1$.

Recall that for any integers k and m we denote by $k \bmod m$ the congruence class $k + m\mathbb{Z}$ of k modulo m. Set

$$\Gamma' = \begin{cases} \{\, k \bmod p^n \in (\mathbb{Z}/p^n\mathbb{Z})^* \,|\, k \in \mathbb{Z},\ k \equiv 1 \pmod{p} \,\} & \text{if } p \neq 2 \text{ and } n \geqslant 1, \\ \{\, k \bmod p^n \in (\mathbb{Z}/2^n\mathbb{Z})^* \,|\, k \in \mathbb{Z},\ k \equiv 1 \pmod{4} \,\} & \text{if } p = 2 \text{ and } n \geqslant 2. \end{cases}$$

Using the considerations above, it follows that, if $p \neq 2$, then

$$\Gamma \cong \Gamma' \times (pG)^{\perp} \text{ is cyclic of order } p^{n-1}t, \text{ with } t \,|\, (p-1),$$

and if $p \neq 2$, then $G^{\perp} = (2G)^{\perp} = \{1\}$ and

$$\Gamma = (\mathbb{Z}/2^n\mathbb{Z})^* \cong \Gamma' \times \{1 \bmod 2^n, -1 \bmod 2^n\} \cong \mathbb{Z}/2^{n-2}\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

Observe that if $\Gamma' = \{1\}$, then, for $p \neq 2$,

$$\Gamma \cong \mathbb{Z}/t\mathbb{Z} \text{ is a nontrivial subgroup of } \mathbb{F}_p^*,\ G = Z^1(\Gamma, \mathbb{F}_p) = B^1(\Gamma, \mathbb{F}_p) = B_p,$$

while, for $p = 2$,

$$G = Z^1((\mathbb{Z}/4\mathbb{Z})^*, \mathbb{Z}/4\mathbb{Z}) = B_4 = \langle \varepsilon_4' \rangle,$$

as desired.

Now assume that $\Gamma' \neq \{1\}$, i.e., $n \geqslant 2$ for $p \neq 2$, and $n \geqslant 3$ for $p = 2$. Set $\widetilde{G'} = \mathrm{res}^{\Gamma}_{\Gamma'}(G) = \langle g|_{\Gamma'} \rangle$. Note that $\widetilde{G'}^{\perp} = G^{\perp} \cap \Gamma' = \{1\}$ since $G^{\perp} \cap \Gamma' \subseteq (pG)^{\perp} \cap \Gamma' = \{1\}$ for $p \neq 2$, and $G^{\perp} = \{1\}$ for $p = 2$. As $1 < |\Gamma'| = (\Gamma' : \widetilde{G'}^{\perp}) \leqslant |\widetilde{G'}|$, it follows that $\widetilde{G'} \neq \{0\}$ and $\Gamma'^{\perp} \cap G \neq G$; hence $\Gamma'^{\perp} \cap G \in \mathcal{K}(\Gamma, A)$. By Proposition 1.8, it follows that $\widetilde{G'} \in \mathcal{N}(\Gamma', A)$, i.e., $p^{n-1} = (\Gamma' : \widetilde{G'}^{\perp}) < |\widetilde{G'}| \,|\, |G| = p^n$ if $p \neq 2$, and $2^{n-2} = (\Gamma' : \widetilde{G'}^{\perp}) < |\widetilde{G'}| \,|\, |G| = 2^n$ if $p = 2$. Consequently, for $p \neq 2$ we have

$\widetilde{G'} \cong G \cong \mathbb{Z}/p^n\mathbb{Z}$, and for $p = 2$ we have either $\widetilde{G'} \cong \mathbb{Z}/2^{n-1}\mathbb{Z}$ or $\widetilde{G'} \cong G \cong \mathbb{Z}/2^n\mathbb{Z}$. Thus we arrived to a contradiction since

$$Z^1(\Gamma', A) = B^1(\Gamma', A) \cong \begin{cases} \mathbb{Z}/p^{n-1}\mathbb{Z} & \text{if } p \neq 2, \\ \mathbb{Z}/2^{n-2}\mathbb{Z} & \text{if } p = 2. \end{cases}$$

Indeed, let

$$\sigma = \begin{cases} (1+p) \bmod p^n & \text{if } \ p \neq 2 \\ 5 \bmod 2^n & \text{if } \ p = 2 \end{cases}$$

be the canonical generator of the cyclic group Γ'. The injective group morphism

$$Z^1(\Gamma', A) \longrightarrow A, \, h \mapsto h(\sigma),$$

maps $Z^1(\Gamma', A)$ onto $\mathrm{Ker}(N)$ and $B^1(\Gamma', A)$ onto $T(A)$, where $N : A \longrightarrow A$ is the norm sending $a \in A = (1/p^n)\mathbb{Z}/\mathbb{Z}$ to $\widetilde{N}a$,

$$\widetilde{N} = \begin{cases} \displaystyle\sum_{i=0}^{p^{n-1}-1} (1+p)^i & \text{if } \ p \neq 2, \\ \displaystyle\sum_{i=0}^{2^{n-2}-1} 5^i & \text{if } \ p = 2, \end{cases}$$

and

$$T : A \longrightarrow A, \, a \mapsto \sigma a - a = \begin{cases} p\,a & \text{if } \ p \neq 2, \\ 4\,a & \text{if } \ p = 2. \end{cases}$$

Now, it is easily checked by induction that the p-adic valuation of the natural number $\widetilde{N}$ is $n-1$ for $p \neq 2$ and $n-2$ for $p = 2$. This implies that

$$\mathrm{Ker}(N) = T(A) = \begin{cases} pA \cong \mathbb{Z}/p^{n-1}\mathbb{Z} & \text{if } \ p \neq 2, \\ 4A \cong \mathbb{Z}/2^{n-2}\mathbb{Z} & \text{if } \ p = 2, \end{cases}$$

as desired. □

The next statement, which is an equivalent form of Lemma 1.12, is actually an abstract version of the Kneser Criterion [10] from the field theoretic Cogalois Theory. Note that the place of the primitive p-th roots of unity ζ_p, p odd prime, from the Kneser Criterion [10] is taken in its abstract version by ε_p, while ε'_4 corresponds to $1 - \zeta_4$.

Theorem 1.13. (The Abstract Kneser Criterion). *The following assertions are equivalent for $G \leqslant Z^1(\Gamma, A)$.*

(1) *G is a Kneser group of $Z^1(\Gamma, A)$.*

(2) *$\varepsilon_p \notin G$ whenever $4 \neq p \in \mathcal{P}(\Gamma, A)$ and $\varepsilon'_4 \notin G$ whenever $4 \in \mathcal{P}(\Gamma, A)$.*

Proof. (1) $\Longrightarrow$ (2): Assume that $G \in \mathcal{K}(\Gamma, A)$. If $\varepsilon_p \in G$ for some $4 \neq p \in \mathcal{P}(\Gamma, A)$, then $B_p = \langle \varepsilon_p \rangle \leqslant G$, hence $B_p \in \mathcal{K}(\Gamma, A)$, which contradicts Lemma 1.12. Similarly, if $4 \in \mathcal{P}(\Gamma, A)$ and $\varepsilon'_4 \in G$ then $B_4 = \langle \varepsilon'_4 \rangle \leqslant G$, hence $B_4 \in \mathcal{K}(\Gamma, A)$, which again contradicts Lemma 1.12.

(2) $\Longrightarrow$ (1): Assume that $G \notin \mathcal{K}(\Gamma, A)$, i.e., $G \in \mathcal{N}(\Gamma, A)$. Then G contains a minimal member of $\mathcal{N}(\Gamma, A)$, i.e., an element of the set $\mathcal{N}(\Gamma, A)_{\min}$. To conclude, apply now Lemma 1.12. □

Corollary 1.14. *$Z^1(\Gamma, A)$ is a Kneser group of itself if and only if $\mathcal{P}(\Gamma, A) = \varnothing$.* □

2 Cogalois groups of cocycles

In this section we define the concept of abstract Cogalois group and establish various equivalent characterizations for them, including a *Quasi-Purity Criterion*.

For a given subgroup G of $Z^1(\Gamma, A)$, the lattice $\mathbb{L}(G)$ of all subgroups of G and the lattice $\overline{\mathbb{L}}(\Gamma | G^{\perp})$ of all closed subgroups of Γ lying over $G^{\perp}$ are related through the canonical order-reversing maps $H \mapsto H^{\perp}$ and $\Delta \mapsto G \cap \Delta^{\perp} = G \cap \operatorname{Ker}(\operatorname{res}^{\Gamma}_{\Delta})$. Clearly, these two maps establish a Galois connection, which is induced by the one considered in Proposition 0.1 (1).

Definition 2.1. *A subgroup G of $Z^1(\Gamma, A)$ is said to be a* Cogalois group *of $Z^1(\Gamma, A)$ if it is a Kneser group of $Z^1(\Gamma, A)$ and the maps $(-)^{\perp}$ between $\mathbb{L}(G)$ and $\overline{\mathbb{L}}(\Gamma | G^{\perp})$ are lattice anti-isomorphisms inverse to one another.* □

Some characterizations of Cogalois groups of $Z^1(\Gamma, A)$ are given in the next result.

Proposition 2.2. *The following statements are equivalent for a Kneser group G of $Z^1(\Gamma, A)$.*

(1) $\Delta = (G \cap \Delta^{\perp})^{\perp}$ *for every* $\Delta \in \overline{\mathbb{L}}(\Gamma | G^{\perp})$.

(2) $\operatorname{res}^{\Gamma}_{\Delta}(G) \in \mathcal{K}(\Delta, A)$ *for every* $\Delta \in \overline{\mathbb{L}}(\Gamma | G^{\perp})$.

(3) *The map* $\mathbb{L}(G) \longrightarrow \overline{\mathbb{L}}(\Gamma | G^{\perp})$, $H \mapsto H^{\perp}$, *is onto.*

(4) *The map* $\overline{\mathbb{L}}(\Gamma | G^{\perp}) \longrightarrow \mathbb{L}(G)$, $\Delta \mapsto G \cap \Delta^{\perp}$, *is injective.*

(5) *G is a Cogalois group of $Z^1(\Gamma, A)$.*

Proof. (1) $\Longleftrightarrow$ (2) by Corollary 1.7.

(1) $\Rightarrow$ (3): For any $\Delta \in \overline{\mathbb{L}}(\Gamma | G^{\perp})$, we have $\Delta = H^{\perp}$, where $H = G \cap \Delta^{\perp} \in \mathbb{L}(G)$.

(3) $\Rightarrow$ (4): Let $\Delta_1, \Delta_2 \in \overline{\mathbb{L}}(\Gamma | G^{\perp})$ be such that $G \cap \Delta_1^{\perp} = G \cap \Delta_2^{\perp}$. By assumption, $\Delta_1 = H_1^{\perp}$, $\Delta_2 = H_2^{\perp}$ for some $H_1, H_2 \in \mathbb{L}(G)$. By Lemma 1.5, $H_1 = G \cap H_1^{\perp\perp} = G \cap \Delta_1^{\perp} = G \cap \Delta_2^{\perp} = G \cap H_2^{\perp\perp} = H_2$, and hence, $\Delta_1 = \Delta_2$, as desired.

(4) $\Rightarrow$ (5): For any $H \in \mathbb{L}(G)$, we have $G \cap H^{\perp\perp} = H$ by Lemma 1.5, so the composition of the canonical maps $\mathbb{L}(G) \longrightarrow \overline{\mathbb{L}}(\Gamma|G^{\perp}) \longrightarrow \mathbb{L}(G)$ is the identity. It follows that the map $\Delta \mapsto G \cap \Delta^{\perp}$ is onto, and hence bijective, with inverse $H \mapsto H^{\perp}$. Thus, the canonical maps above are anti-isomorphisms of posets, and consequently, also anti-isomorphisms of lattices inverse to one another, as desired.

(5) $\Rightarrow$ (1): Let $\Delta \in \overline{\mathbb{L}}(\Gamma|G^{\perp})$. Then, by assumption, there exists a unique $H \in \mathbb{L}(G)$ such that $\Delta = H^{\perp}$ and $H = G \cap \Delta^{\perp}$; hence $\Delta = (G \cap \Delta^{\perp})^{\perp}$, as required. □

As $\Gamma \in \overline{\mathbb{L}}(\Gamma|G^{\perp})$ for every $G \leqslant Z^1(\Gamma, A)$ and $\mathcal{P}(\Delta, A) \subseteq \mathcal{P}(\Gamma, A)$ for all $\Delta \in \overline{\mathbb{L}}(\Gamma)$, the next result follows immediately from Proposition 2.2 and Corollary 1.14.

Corollary 2.3. *A subgroup G of $Z^1(\Gamma, A)$ is Cogalois if and only if $\mathrm{res}^{\Gamma}_{\Delta}(G)$ is a Kneser group of $Z^1(\Delta, A)$ for every $\Delta \in \overline{\mathbb{L}}(\Gamma|G^{\perp})$.*

In particular, $Z^1(\Gamma, A)$ is a Cogalois group of itself if and only if $Z^1(\Gamma, A)$ is a Kneser group of itself. □

Definition 2.4. *A subgroup D of an Abelian group C is said to be* quasi n-pure, *where n is a given positive integer, if $C[n] \subseteq D$, or equivalently $C[n] = D[n]$. For $M \subseteq \mathbb{N}$, C is* quasi M-pure *if C is quasi n-pure for all $n \in M$.*

Recall that a well established concept in Group Theory is that of *n-purity*: a subgroup D of an Abelian group C is said to be *n-pure* if $D \cap nC = nD$. There is no connection between the concepts of n-purity and quasi n-purity; e.g., the subgroup $2\mathbb{Z}/4\mathbb{Z}$ of $\mathbb{Z}/4\mathbb{Z}$ is quasi 2-pure but not 2-pure, and any of the three subgroups of order 2 of the dihedral group $\mathbb{D}_4$ is 2-pure but not quasi 2-pure. Notice that the abstract notion of quasi n-purity goes back to the concept of n-purity from the field theoretic Cogalois Theory (see Albu [1], Albu and Nicolae [6]).

For any subgroup G of $Z^1(\Gamma, A)$ we denote $\mathcal{P}_G := \mathcal{O}_G \cap \mathcal{P}$, i.e., $\mathcal{P}_G$ is the set of those $p \in \mathcal{P}$ for which $\exp(G[p]) = p$.

The quasi $\mathcal{P}_G$-purity plays a basic role in the characterization of Cogalois groups of $Z^1(\Gamma, A)$. The next result is the abstract version of the *General Purity Criterion* [1], Theorem 2.3, from the field theoretic infinite Cogalois Theory.

Theorem 2.5. (The Quasi-Purity Criterion). *The following statements are equivalent for a subgroup G of $Z^1(\Gamma, A)$.*

(1) *G is Cogalois.*

(2) *The subgroup A^{Γ} of $A^{G^{\perp}}$ is quasi $\mathcal{P}_G$-pure.*

(3) *$G^{\perp} \not\subseteq \varepsilon_p^{\perp}$ for all $p \in \mathcal{P}_G \cap \mathcal{P}(\Gamma, A)$.*

Proof. (2) $\Longrightarrow$ (3): Let $p \in \mathcal{P}_G \cap \mathcal{P}(\Gamma, A)$. Then $\widehat{1/p} \in A \setminus A^{\Gamma}$, and hence $\widehat{1/p} \notin A^{G^{\perp}}$, as $A^{G^{\perp}}[p] = A^{\Gamma}[p]$ by hypothesis. Consequently, there exists $\sigma \in G^{\perp}$ such that $\sigma\,\widehat{1/p} \neq \widehat{1/p}$, i.e., $\sigma \notin \varepsilon_p^{\perp}$, which shows that $G^{\perp} \not\subseteq \varepsilon_p^{\perp}$, as desired.

(3) $\Longrightarrow$ (2): Let $p \in \mathcal{P}_G$. Then clearly $\widehat{1/p} \in A$. Assuming $\widehat{1/p} \in A^{\Gamma}$, we obtain that $A^{\Gamma}[p] = A^{G^{\perp}}[p] = (1/p)\mathbb{Z}/\mathbb{Z}$, as desired. Now assume that $\widehat{1/p} \notin A^{\Gamma}$.

Since $G^{\perp} \not\subseteq \varepsilon_p^{\perp}$ by hypothesis, it follows that $A^{\Gamma}[p] = A^{G^{\perp}}[p] = \{0\}$ for $p \neq 4$, and $A^{\Gamma}[p] = A^{G^{\perp}}[p] = (1/2)\mathbb{Z}/\mathbb{Z}$ for $p = 4$.

(1) $\Longrightarrow$ (3): Suppose that G is Cogalois, and let $p \in \mathcal{P}_G \cap \mathcal{P}(\Gamma, A)$. Then $\widehat{1/p} \in A \setminus A^{\Gamma}$, and there exists a cocycle $h \in G$ of order p. Let $H \cong \mathbb{Z}/p\mathbb{Z}$ denote the subgroup of G generated by h. Since G is a Kneser group of $Z^1(\Gamma, A)$, $(\Gamma : H^{\perp}) = |H| = p$. Assuming that $G^{\perp} \subseteq \varepsilon_p^{\perp}$, we have to derive a contradiction. We distinguish the following two cases:

Case (i): $p \in \mathbb{P} \setminus \{2\}$. Since $G \in \mathcal{K}(\Gamma, A)$, it follows by Theorem 1.13 that $\varepsilon_p \notin G$. Setting $\alpha := h - \varepsilon_p \in Z^1(\Gamma, (1/p)\mathbb{Z}/\mathbb{Z}) \setminus G$, we deduce that $\operatorname{ord}(\alpha) = p$ and $\langle \varepsilon_p \rangle \cap \langle \alpha \rangle = \{0\}$. Consequently, again by Theorem 1.13., $\langle \alpha \rangle \in \mathcal{K}(\Gamma, A)$, and hence $(\Gamma : \alpha^{\perp}) = p$. Since $G^{\perp} \leqslant h^{\perp}$ and $G^{\perp} \leqslant \varepsilon_p^{\perp}$ by assumption, it follows that $G^{\perp} \leqslant \alpha^{\perp}$. As G is Cogalois, we deduce that $\alpha^{\perp} = (G \cap \alpha^{\perp\perp})^{\perp}$ and $|G \cap \alpha^{\perp\perp}| = (\Gamma : \alpha^{\perp}) = p$, therefore $G \cap \alpha^{\perp\perp} \cong \mathbb{Z}/p\mathbb{Z}$. Now consider the subgroup $H' := H + (G \cap \alpha^{\perp\perp})$ of G. As p is a prime number, it follows that either $H' = H \cong \mathbb{Z}/p\mathbb{Z}$ or $H' = H \oplus (G \cap \alpha^{\perp\perp}) \cong (\mathbb{Z}/p\mathbb{Z}) \oplus (\mathbb{Z}/p\mathbb{Z})$. Since $H' \leqslant G \in \mathcal{K}(\Gamma, A)$, we deduce that $(\Gamma : H'^{\perp}) \in \{p, p^2\}$. This implies that $(\Gamma : \varepsilon_p^{\perp}) \,|\, p^2$ since $H'^{\perp} \leqslant h^{\perp} \cap \alpha^{\perp} \leqslant \varepsilon_p^{\perp}$. On the other hand, $\varepsilon_p^{\perp}$ is the kernel of the (nontrivial) action of Γ on $A[p] = (1/p)\mathbb{Z}/\mathbb{Z}$, and hence $2 \leqslant (\Gamma : \varepsilon_p^{\perp}) \,|\, (p-1)$, which is a contradiction.

Case (ii): $p = 4$. Let $\varepsilon_4' \in Z^1(\Gamma, A[4]) = Z^1(\Gamma, (1/4)\mathbb{Z}/\mathbb{Z})$ be the 1-cocycle defined in Section 1, and remember that $\varepsilon_4 = 2\varepsilon_4'$. As $\widehat{1/4} \notin A^{\Gamma}$, the action of Γ on $A[4] = (1/4)\mathbb{Z}/\mathbb{Z}$, whose kernel is $\varepsilon_4^{\perp} = \varepsilon_4'^{\perp}$, is nontrivial, and hence $\Gamma/\varepsilon_4^{\perp} \cong (\mathbb{Z}/4\mathbb{Z})^* \cong \mathbb{Z}/2\mathbb{Z}$, i.e., $(\Gamma : \varepsilon_4^{\perp}) = 2$. Since G is Cogalois and $G^{\perp} \leqslant \varepsilon_4^{\perp}$ by assumption, it follows that $\varepsilon_4^{\perp} = (G \cap \varepsilon_4^{\perp\perp})^{\perp}$ and $|G \cap \varepsilon_4^{\perp\perp}| = (\Gamma : \varepsilon_4^{\perp}) = 2$, i.e., $G \cap \varepsilon_4^{\perp\perp} \cong \mathbb{Z}/2\mathbb{Z}$. One easily checks that ε_4 is the unique element of order 2 of $\varepsilon_4^{\perp\perp}$, and hence $G \cap \varepsilon_4^{\perp\perp} = \langle \varepsilon_4 \rangle$, in particular, $\varepsilon_4 \in G$. On the other hand, since $G \in \mathcal{K}(\Gamma, A)$, it follows by Theorem 1.13 that $\varepsilon_4' \notin G$, and hence $h \notin \{\varepsilon_4', -\varepsilon_4'\}$. Set $\beta := h - \varepsilon_4'$ and $H_1 := \langle h, \varepsilon_4 \rangle \leqslant G$. Then $0 \neq \beta \notin \langle \varepsilon_4' \rangle$. Two subcases arise:

Subcase (1): $\varepsilon_4 \in H$. Then $2h = \varepsilon_4$ and $2\beta = 2h - 2\varepsilon_4' = 2h - \varepsilon_4 = 0$, i.e., $\operatorname{ord}(\beta) = 2$. By Lemma 1.1, we have $(\Gamma : \beta^{\perp}) \leqslant |\langle \beta \rangle| = 2$. Observe that $\beta^{\perp} \neq \Gamma$, for otherwise, we would have $0 \neq \beta \in \beta^{\perp\perp} = \Gamma^{\perp} = \{0\}$, which is a contradiction. Thus, $(\Gamma : \beta^{\perp}) = 2$. On the other hand, $G^{\perp} \leqslant H^{\perp} = H^{\perp} \cap \varepsilon_4^{\perp} = h^{\perp} \cap \varepsilon_4'^{\perp} \leqslant \beta^{\perp}$, and hence $G \cap \beta^{\perp\perp} \leqslant G \cap H^{\perp\perp} = H$, $\beta^{\perp} = (G \cap \beta^{\perp\perp})^{\perp}$, and $|G \cap \beta^{\perp\perp}| = (\Gamma : \beta^{\perp}) = 2$, as G is Cogalois. Since $\langle \varepsilon_4 \rangle$ is the unique subgroup of order 2 of $H \cong \mathbb{Z}/4\mathbb{Z}$, it follows that $G \cap \beta^{\perp\perp} = \langle \varepsilon_4 \rangle$. Therefore $\beta \in (\beta^{\perp})^{\perp} = ((G \cap \beta^{\perp\perp})^{\perp})^{\perp} = \varepsilon_4^{\perp\perp}$, so $\beta = \varepsilon_4$ since $\operatorname{ord}(\beta) = 2$ and ε_4 is the unique element of order 2 contained in $\varepsilon_4^{\perp\perp}$. In particular, $\beta \in G$, and hence $\varepsilon_4' = h - \beta \in G$, which is a contradiction.

Subcase (2): $\varepsilon_4 \notin H$. Then $H_1 = H \oplus \langle \varepsilon_4 \rangle \cong \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. Since $2\beta = 2h - \varepsilon_4 \neq 0$ and $4\beta = 0$, it follows that $\operatorname{ord}(\beta) = 4$. But $\varepsilon_4' \notin \langle \beta \rangle$, so $\langle \beta \rangle \in \mathcal{K}(\Gamma, A)$ by Theorem 1.13, and then, $(\Gamma : \beta^{\perp}) = 4$. Since $H_1 \leqslant G, G^{\perp} \leqslant H_1^{\perp} = h^{\perp} \cap \varepsilon_4^{\perp} = h^{\perp} \cap \varepsilon_4'^{\perp} \leqslant \beta^{\perp}$, and G is Cogalois, it follows that $H_2 := G \cap \beta^{\perp\perp} \leqslant G \cap H_1^{\perp\perp} = H_1$, $H_2^{\perp} = \beta^{\perp}$, and $|H_2| = (\Gamma : \beta^{\perp}) = 4$. Thus, H_2 is a subgroup of order 4 of H_1. Setting $H_3 = H_2 + \langle \varepsilon_4 \rangle$, we deduce that $H_3^{\perp} = H_2^{\perp} \cap \varepsilon_4^{\perp} = \beta^{\perp} \cap \varepsilon_4'^{\perp} \leqslant h^{\perp} \cap \varepsilon_4^{\perp} = H_1^{\perp} \leqslant H_2^{\perp} \cap \varepsilon_4^{\perp}$, so $H_3^{\perp} = H_1^{\perp}$, and hence $H_3 = H_1$ as G is Cogalois and $H_1 + H_3 \leqslant G$. Since $H_1 = H \oplus \langle \varepsilon_4 \rangle \cong \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ and $|H_2| = 4$, we deduce that $H_2 \cong \mathbb{Z}/4\mathbb{Z}$, and hence either $H_2 = H$ or $H_2 = \langle h - \varepsilon_4 \rangle$. Assuming that $H_2 = H$, it follows that $(h - \varepsilon_4')^{\perp} = \beta^{\perp} = H_2^{\perp} = H^{\perp} = h^{\perp}$. Therefore $H^{\perp} \leqslant \varepsilon_4'^{\perp} = \varepsilon_4^{\perp}$, and so $\varepsilon_4 \in G \cap \varepsilon_4^{\perp\perp} \leqslant G \cap H^{\perp\perp} = H$, which is a contradiction. Thus, it remains only to consider the case $H_2 = \langle h - \varepsilon_4 \rangle$. Then $(h - \varepsilon_4')^{\perp} = \beta^{\perp} = H_2^{\perp} = (h - \varepsilon_4)^{\perp}$. Replacing β with $h + \varepsilon_4'$ and proceeding as above, we finally obtain that $(h + \varepsilon_4')^{\perp} = (h - \varepsilon_4)^{\perp} = (h - \varepsilon_4')^{\perp}$, and hence $\Gamma \setminus \varepsilon_4^{\perp} \subseteq h^{\perp}$, as one easily checks. On the other hand, since $(\Gamma : \varepsilon_4^{\perp}) = 2$, it follows that $\Gamma = \varepsilon_4^{\perp} \cup \sigma\, \varepsilon_4^{\perp}$ for some (for all) $\sigma \in \Gamma \setminus \varepsilon_4^{\perp}$. Consequently, for every $\tau \in \varepsilon_4^{\perp}$ and $\sigma \in \Gamma \setminus \varepsilon_4^{\perp}$ we have $0 = h(\sigma\tau) = h(\sigma) + \sigma h(\tau) = \sigma h(\tau)$, and hence $\varepsilon_4^{\perp} \leqslant h^{\perp}$. Thus $h^{\perp} = \Gamma$, i.e., $h = 0$, which is a contradiction.

(3) $\Longrightarrow$ (1): Using Corollary 2.3, we have to show that $\widetilde{G} := \mathrm{res}^{\Gamma}_{\Delta}(G) \in \mathcal{K}(\Delta, A)$ for every $\Delta \in \mathbb{L}(\Gamma | G^{\perp})$. Assuming the contrary, it follows by Theorem 1.13 that there exist $\Delta \in \mathbb{L}(\Gamma | G^{\perp})$ and $p \in \mathcal{P}(\Delta, A) \subseteq \mathcal{P}(\Gamma, A)$, i.e., $\widehat{1/p} \in A \setminus A^{\Delta} \subseteq A \setminus A^{\Gamma}$, such that $\varepsilon_p|_{\Delta} \in \widetilde{G}$ if $p \neq 4$ and $\varepsilon_4'|_{\Delta} \in \widetilde{G}$ if $p = 4$. Consequently, there exists $h \in G$ such that $h|_{\Delta} = \varepsilon_p|_{\Delta}$ if $p \neq 4$, and $h|_{\Delta} = \varepsilon_4'|_{\Delta}$ if $p = 4$. Let $n = \mathrm{ord}(h)$. Since $\mathrm{ord}(\varepsilon_p|_{\Delta}) = p$ for $p \neq 4$ and $\mathrm{ord}(\varepsilon_4'|_{\Delta}) = 4$ for $p = 4$, as $\widehat{1/p} \in A \setminus A^{\Delta}$, it follows that $p \,|\, n$, and hence $p \in \mathcal{P}_G \cap \mathcal{P}(\Gamma, A)$. On the other hand, $G^{\perp} \leqslant h^{\perp} \cap \Delta \leqslant \varepsilon_p^{\perp}$, contrary to our hypothesis. $\square$

Let $\mathcal{C}(\Gamma, A)$ denote the Γ-poset of all Cogalois groups of $Z^1(\Gamma, A)$. The next result shows that $\mathcal{C}(\Gamma, A)$ is a lower Γ-poset, and moreover, the property of a subgroup of $Z^1(\Gamma, A)$ being Cogalois is, like the property of a subgroup of $Z^1(\Gamma, A)$ being Kneser, a property of finitary character.

Corollary 2.6. *The following assertions are equivalent for a subgroup G of $Z^1(\Gamma, A)$.*

(1) $G \in \mathcal{C}(\Gamma, A)$.

(2) $H \in \mathcal{C}(\Gamma, A)$ *for all* $H \leqslant G$.

(3) $H \in \mathcal{C}(\Gamma, A)$ *for all finite* $H \leqslant G$.

Proof. (1) $\Longrightarrow$ (2): Let $H \leqslant G$ and $p \in \mathcal{P}_H \cap \mathcal{P}(\Gamma, A)$. Then clearly $p \in \mathcal{P}_G \cap \mathcal{P}(\Gamma, A)$, hence $G^{\perp} \not\subseteq \varepsilon_p^{\perp}$ by Theorem 2.5, and then we also have $H^{\perp} \not\subseteq \varepsilon_p^{\perp}$ since $G^{\perp} \subseteq H^{\perp}$. Using again Theorem 2.5, we deduce that $H \in \mathcal{C}(\Gamma, A)$.

(2) $\Longrightarrow$ (3) is obvious.

(3) $\Longrightarrow$ (1): Let $p \in \mathcal{P}(\Gamma, A) \cap \mathcal{P}_G$. Choose some $h \in G$ of order p, and set $G_g = \langle g, h \rangle$ for any $g \in G$. By Theorem 2.5, it follows that the family of closed subsets $(G_g^{\perp} \setminus \varepsilon_p^{\perp})_{g \in G}$ of Γ has the finite intersection property, therefore, by compactness, their intersection $G^{\perp} \setminus {\varepsilon_p}^{\perp}$ is nonempty, as desired. $\square$

Corollary 2.7. *Let p be an odd prime number, and let G be a p-subgroup of $Z^1(\Gamma, A)$. Then G is Cogalois if and only if G is Kneser.*

Proof. By Definition 1.4 and Corollary 2.6 we may assume that the p-group G is finite. Assume that G is Kneser and prove that G is Cogalois with the aid of Theorem 2.5. Of course, we may assume that $p \in \mathcal{P}(\Gamma, A)$, for otherwise we have nothing to prove. As we have already seen at the beginning of the proof of Lemma 1.12, the index $(\Gamma : \varepsilon_p^{\perp})$ is a divisor $\neq 1$ of $p-1$, in particular it is prime to p. Since the p-group G is Kneser, it follows that $(\Gamma : G^{\perp}) = |G|$ is a power of p, and hence $G^{\perp} \not\subseteq \varepsilon_p^{\perp}$, as desired. □

Remarks 2.8. (1) Corollary 2.7 may fail for $p = 2$. Indeed the simplest example of a Kneser non-Cogalois 2-group is the one corresponding to the action of type D_4 or D_8 (see Definition 2.14 and Lemma 2.15).

(2) In contrast with the property of Kneser groups given in Corollary 1.11, the condition that all p-primary components of G are Cogalois, is in general not sufficient to ensure G being Cogalois. To see that, observe that the group corresponding to the action of type D_{pr} is Kneser but not Cogalois, and has all its primary components Cogalois (see again Definition 2.14 and Lemma 2.15).

(3) By Zorn's Lemma, for any $G \in \mathcal{C}(\Gamma, A)$ there exists a maximal element M of $\mathcal{C}(\Gamma, A)$ such that $G \subseteq M$. □

The next theorem essentially shows that a subgroup $G \leqslant Z^1(\Gamma, A)$ is Cogalois if and only if G has a prescribed structure, and is the abstract version of the structure theorem [1], Theorem 4.3, for Kneser groups from the field theoretic infinite Cogalois Theory.

For any subgroup G of $Z^1(\Gamma, A)$ and for any prime number p, denote

$$\widetilde{G}_p = \begin{cases} G^{\perp\perp}(p) & \text{if either } p \in \mathcal{P}_G, \text{ or } p = 2 \text{ and } 4 \in \mathcal{P}_G, \\ G^{\perp\perp}[2] & \text{if } p = 2,\ 4 \notin \mathcal{P}_G, \text{ and } G[2] \neq 0, \\ 0 & \text{otherwise,} \end{cases}$$

and

$$\widetilde{G} = \bigoplus_{p \in \mathbb{P}} \widetilde{G}_p .$$

Now, consider the subgroup

$$\mu_G = \bigcup_{n \in \mathcal{O}_G} (1/n)\mathbb{Z}/\mathbb{Z} = \sum_{h \in G} h(\Gamma) = \bigoplus_{p \in \mathbb{P}} \Big(\bigcup_{h \in G(p)} h(\Gamma) \Big)$$

of A, and let $Z^1(\Gamma \,|\, G^{\perp}, \mu_G) = G^{\perp\perp} \cap Z^1(\Gamma, \mu_G)$ denote the subgroup of $Z^1(\Gamma, A)$ consisting of those cocycles which are trivial on $G^{\perp}$ and take values in μ_G. Clearly,

$$G \leqslant Z^1(\Gamma \,|\, G^{\perp}, \mu_G) \leqslant \widetilde{G} \leqslant G^{\perp\perp},$$

which implies that

$$G^{\perp} = Z^1(\Gamma \,|\, G^{\perp}, \mu_G)^{\perp} = \widetilde{G}^{\perp}.$$

Notice also that

$$\mathcal{P}_G = \mathcal{P}_{Z^1(\Gamma \,|\, G^{\perp}, \mu_G)} = \mathcal{P}_{\widetilde{G}} .$$

Theorem 2.9. *With the notation above, the following assertions are equivalent for a Kneser group G of $Z^1(\Gamma, A)$.*

(1) *G is Cogalois.*

(2) $G = Z^1(\Gamma \,|\, G^{\perp}, \mu_G)$.

(3) $G = \widetilde{G}$.

Proof. (1) $\Longrightarrow$ (3): If G is Cogalois, then $\widetilde{G}$ is also Cogalois by Theorem 2.5 since $\mathcal{P}_G = \mathcal{P}_{\widetilde{G}}$ and $G^{\perp} = \widetilde{G}^{\perp}$. Therefore, by the definition of the concept of Cogalois group, we have $H = \widetilde{G} \cap H^{\perp\perp}$ for any $H \in \mathbb{L}(\widetilde{G})$. In particular, we deduce that $G = \widetilde{G} \cap G^{\perp\perp} = \widetilde{G}$, as desired.

(3) $\Longrightarrow$ (2) is trivial.

(2) $\Longrightarrow$ (1): Assume that $G = Z^1(\Gamma \,|\, G^{\perp}, \mu_G)$ and G is not Cogalois. Then, by Theorem 2.5, there exists $p \in \mathcal{P}_G \cap \mathcal{P}(\Gamma, A)$ such that $G^{\perp} \subseteq \varepsilon_p^{\perp}$. Therefore, $\varepsilon_p \in Z^1(\Gamma \,|\, G^{\perp}, \mu_G) = G$ for $p \neq 4$, and $\varepsilon_4' \in Z^1(\Gamma \,|\, G^{\perp}, \mu_G) = G$ for $p = 4$. By Theorem 1.13, we deduce that G is not a Kneser group, contrary to our hypothesis. $\square$

Recall that by $\mathcal{C}(\Gamma, A)$ we have denoted the Γ-poset of all Cogalois groups of $Z^1(\Gamma, A)$.

Corollary 2.10. *The map $\mathcal{C}(\Gamma, A) \longrightarrow \overline{\mathbb{L}}(\Gamma), G \mapsto G^{\perp}$, is injective.*

Proof. Let G, $H \in \mathcal{C}(\Gamma, A)$ be such that $G^{\perp} = H^{\perp}$, and prove that $G = H$. By the definition of the groups $\widetilde{G}$ and $\widetilde{H}$, and using Theorem 2.9, it suffices to show that $\mathcal{P}_G = \mathcal{P}_H$ and the groups $G[2]$ and $H[2]$ are simultaneously trivial or not whenever $4 \notin \mathcal{P}_G$. Let $p \in \mathcal{P}_G$ and g a cocycle in G of order p. Since G is Cogalois, we have $(\Gamma : g^{\perp}) = p$, and moreover, there exists only one proper subgroup (of index 2) lying over $g^{\perp}$ if $p = 4$. Since H is also Cogalois and $g^{\perp}$ lies over $H^{\perp}$, it follows that $H \cap g^{\perp\perp}$ is a cyclic subgroup of order p of H, and hence $p \in \mathcal{P}_H$, as desired. The latter condition follows with a similar argument. $\square$

Remark 2.11. An alternative proof of Corollary 2.10 can be done using the following fact: if G is Cogalois, then the order/index-preserving map $U \mapsto U^{\perp}$ maps bijectively the cyclic subgroups of G (which are the only finite subgroups U of the torsion Abelian group G for which the lattice $\mathbb{L}(U)$ is distributive) onto the open subgroups Δ of Γ lying over $G^{\perp}$ for which the lattice $\mathbb{L}(\Gamma \,|\, \Delta)$ is distributive. In particular, $\mathcal{O}_G$ consists of those positive integers n for which there exists an open subgroup Δ of Γ lying over $G^{\perp}$ such that $(\Gamma : \Delta) = n$ and the lattice $\mathbb{L}(\Gamma \,|\, \Delta)$ is distributive. $\square$

Corollary 2.12. *The following assertions are equivalent for $G \in \mathcal{C}(\Gamma, A)$.*

(1) *G is stable under the action of Γ, i.e., G is a Γ-submodule of $Z^1(\Gamma, A)$.*

(2) $G^{\perp} \lhd \Gamma$.

(3) $\mu_G^{G^{\perp}} = \mu_G$.

Proof. (1) $\Longrightarrow$ (2) holds for any $G \leqslant Z^1(\Gamma, A)$ since $(\sigma G)^{\perp} = \sigma G^{\perp} \sigma^{-1}$ for all $\sigma \in \Gamma$.

(2) $\Longrightarrow$ (3): As $\mu_G = \sum_{g \in G} g(\Gamma)$, we have only to show that $\sigma g(\tau) = g(\tau)$ for all $g \in G$, $\sigma \in G^{\perp}$, $\tau \in \Gamma$. Since, by assumption, $G^{\perp} \lhd \Gamma$, we have $\tau^{-1}\sigma\tau \in G^{\perp}$, so $0 = g(\tau^{-1}\sigma\tau) = \tau^{-1}(\sigma g(\tau) - g(\tau))$, and hence $\sigma g(\tau) = g(\tau)$, as desired. Note that the implication (2) $\Longrightarrow$ (3) also holds for any $G \leqslant Z^1(\Gamma, A)$.

(3) $\Longrightarrow$ (1): Let $g \in G$, $\tau \in \Gamma$, and prove that $\tau g \in G$. Since $G = Z^1(\Gamma \,|\, G^{\perp}, \mu_G)$ by Theorem 2.9, we have to show that $\tau g|_{G^{\perp}} = 0$ and $(\tau g)(\Gamma) \subseteq \mu_G$. From the hypothesis it follows that $(\tau g)(\sigma) = \tau g(\tau^{-1}\sigma\tau) = \sigma g(\tau) - g(\tau) = 0$ for any $\sigma \in G^{\perp}$, as desired. Note that the latter condition holds in general since any subgroup of A, in particular μ_G, is stable under the action of Γ. □

Corollary 2.13. *If $G \in \mathcal{C}(\Gamma, A)$ is a Γ-submodule of $Z^1(\Gamma, A)$, then*

$$G \cong Z^1(\Gamma/G^{\perp}, \mu_G).$$

Proof. Since G is Cogalois, we have $G = Z^1(\Gamma \,|\, G^{\perp}, \mu_G)$ by Theorem 2.9, and since G is a Γ-submodule of $Z^1(\Gamma, A)$, we have $G^{\perp} \lhd \Gamma$ by Corollary 2.12. To conclude, observe that $Z^1(\Gamma \,|\, G^{\perp}, \mu_G) \cong Z^1(\Gamma/G^{\perp}, \mu_G)$. □

According to Lemma 1.12, the Kneser groups are precisely those subgroups of $Z^1(\Gamma, A)$ which do not contain some particular cyclic groups, namely the minimal subgroups B_p which are not Kneser, $p \in \mathcal{P}(\Gamma, A)$. Using Corollary 2.6 we are going to present a similar characterization for Cogalois groups. To do that we will first describe effectively the minimal subgroups of $Z^1(\Gamma, A)$ which are Kneser but not Cogalois. A special class of actions which are introduced below plays a major role in this description.

Definition 2.14. *Let Γ be a finite group, and let A be a finite subgroup of $\mathbb{Q}/\mathbb{Z}$ on which the group Γ acts. One says that the action of Γ on A, or the Γ-module A, is*

(1) *of type* D_4 *if* $\Gamma = \mathbb{D}_4 = \langle \sigma, \tau \,|\, \sigma^2 = \tau^2 = (\sigma\tau)^2 = 1 \rangle \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$,
$A = (1/4)\mathbb{Z}/\mathbb{Z}$, *and* $\sigma\,\widehat{1/4} = -\widehat{1/4}$, $\tau\,\widehat{1/4} = \widehat{1/4}$.

(2) *of type* D_8 *if* $\Gamma = \mathbb{D}_8 = \langle \sigma, \tau \,|\, \sigma^2 = \tau^4 = (\sigma\tau)^2 = 1 \rangle \cong \mathbb{Z}/4\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$,
$A = (1/4)\mathbb{Z}/\mathbb{Z}$, *and* $\sigma\,\widehat{1/4} = -\widehat{1/4}$, $\tau\,\widehat{1/4} = \widehat{1/4}$.

(3) *of type* D_{pr} *if* $\Gamma = \langle \sigma, \tau \,|\, \sigma^r = \tau^p = \sigma\tau\sigma^{-1}\tau^{-u} = 1 \rangle \cong \mathbb{Z}/p\mathbb{Z} \rtimes_u \mathbb{Z}/r\mathbb{Z}$,
$A = (1/pr)\mathbb{Z}/\mathbb{Z}$, *and* $\sigma\widehat{1/pr} = u\widehat{1/pr}$, $\tau\widehat{1/pr} = \widehat{1/pr}$,
where $p \in \mathbb{P}$, $p > 2$, $r \in \mathbb{N}$, $r > 1$, $r \,|\, (p-1)$, *and*
$u \in (\mathbb{Z}/pr\mathbb{Z})^*$ *is such that the order of* $u \bmod p$ *in*
$(\mathbb{Z}/p\mathbb{Z})^*$ *is* r *and* $u \bmod l = 1 \bmod l$ *for all* $l \in \mathcal{P}$, $l \,|\, r$. □

Let $\mathcal{M}(\Gamma, A)$ denote the set (possibly empty) $\mathbb{L}(Z^1(\Gamma, A)) \setminus \mathcal{C}(\Gamma, A)$ of all subgroups of $Z^1(\Gamma, A)$ which are not Cogalois groups. Clearly, for any $G \in \mathcal{M}(\Gamma, A)$ there exists at least one minimal member H of $\mathcal{M}(\Gamma, A)$ such that $H \subseteq G$. By $\mathcal{M}(\Gamma, A)_{\min}$ we shall denote the set of all minimal members of $\mathcal{M}(\Gamma, A)$, and call them *minimal non-Cogalois groups*. Observe that whenever $G \in \mathcal{M}(\Gamma, A)_{\min}$, then necessarily G is a nontrivial finite group according to Corollary 2.6.

Lemma 2.15. *The following conditions are equivalent for any Kneser group G of $Z^1(\Gamma, A)$.*

(1) $G \in \mathcal{M}(\Gamma, A)_{min}$.

(2) $G^{\perp} \lhd \Gamma$ *and the action of* $\Gamma/G^{\perp}$ *on* μ_G *is one of the types* D_4, D_8, *or* D_{pr} *defined as above.*

Proof. (1) $\Longrightarrow$ (2): First assume that the Kneser group G is minimal non-Cogalois. Then, as was observed above, G is finite. As G is not Cogalois, it follows by Theorem 2.5 that there exists $p \in \mathcal{P}(\Gamma, A) \cap \mathcal{P}_G$ such that $G^{\perp} \subseteq \varepsilon_p^{\perp}$. Assume p is minimal with the property above, and let H be a cyclic subgroup of G of order p. Since G is Kneser, its subgroup H is also Kneser, and hence $(\Gamma : H^{\perp}) = |H| = p$, in particular, $H \neq B_p$. We distinguish the following two cases:

Case (i): $p = 4$. We are going to show that $G^{\perp} \lhd \Gamma$ and the action of $\Gamma/G^{\perp}$ on μ_G is either of type D_4 or of type D_8. Two subcases arise:

Subcase (1): $\varepsilon_4 \in H$. As $H \cong \mathbb{Z}/4\mathbb{Z}$ and $H^{\perp} \leqslant \varepsilon_4^{\perp}$, H is not Cogalois by Theorem 2.5, so by the minimality of G we have $G = H \cong \mathbb{Z}/4\mathbb{Z}$ and $\mu_G = (1/4)\mathbb{Z}/\mathbb{Z}$. Since $\sigma g - g \in B^1(\Gamma, \mu_G) = \langle \varepsilon_4 \rangle \leqslant G$ for all $\sigma \in \Gamma, g \in G$, it follows that G is stable under the action of Γ, therefore $G^{\perp} \lhd \Gamma$ and $G \leqslant Z^1(\Gamma/G^{\perp}, \mu_G)$. As the Kneser non-Cogalois group G is cyclic of order 4, it follows that $\Gamma/G^{\perp} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ and the action of $\Gamma/G^{\perp}$ on μ_G is of type D_4.

Subcase (2): $\varepsilon_4 \notin H$. First, show that $\varepsilon_4 \in G$. Since G is Kneser, it follows that $G(2)^{\perp} \leqslant \varepsilon_4^{\perp}$, for otherwise $(G(2)^{\perp} : (G(2)^{\perp} \cap \varepsilon_4^{\perp})) = (\Gamma : \varepsilon_4^{\perp}) = 2$, so $2\,|G(2)| = (\Gamma : (G(2)^{\perp} \cap \varepsilon_4^{\perp}))\,|\,|\Gamma| = |G|$, which is a contradiction. Thus, the 2-primary component $G(2)$ is Kneser, and is not Cogalois by Theorem 2.5. Consequently, by the minimality of G, we deduce that $G = G(2)$. Since $L := \mathrm{res}^{\Gamma}_{\varepsilon_4^{\perp}}(G)$ is a 2-group as a factor of G and $4 \notin \mathcal{P}(\varepsilon_4^{\perp}, A)$, it follows by Theorem 2.5 that L is a Cogalois (in particular, Kneser) group of $Z^1(\varepsilon_4^{\perp}, A)$. Therefore $(G \cap \varepsilon_4^{\perp\perp})^{\perp} = \varepsilon_4^{\perp}$ by Corollary 1.7, so the Kneser group $G \cap \varepsilon_4^{\perp\perp}$ of $Z^1(\Gamma, A)$ is cyclic of order 2. Since the only cocycle of order 2 belonging to $\varepsilon_4^{\perp\perp}$ is ε_4, we deduce that $\varepsilon_4 \in G$, as desired.

Consequently, by the minimality of G, we have $G = H \oplus \langle \varepsilon_4 \rangle \cong \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$, $\mu_G = (1/4)\mathbb{Z}/4\mathbb{Z}$, and $L \cong H \cong \mathbb{Z}/4\mathbb{Z}$. Moreover, since $\varepsilon_4 \in G$, it follows as in the Subcase (1) that G is stable under the action of Γ. Therefore $G^{\perp} \lhd \Gamma$ and G is canonically identified with a subgroup of $Z^1(\Gamma/G^{\perp}, \mu_G)$. In particular, $G^{\perp} \lhd \varepsilon_4^{\perp}$, and $\varepsilon_4^{\perp}/G^{\perp} = \varepsilon_4^{\perp}/L^{\perp} \cong \mathbb{Z}/4\mathbb{Z}$ as $L \cong \mathbb{Z}/4\mathbb{Z}$ is a Cogalois group of $Z^1(\varepsilon_4^{\perp}, A)$. Observe that the canonical action of $H^{\perp}/G^{\perp} \cong \Gamma/\varepsilon_4^{\perp} \cong \mathbb{Z}/2\mathbb{Z}$ on $\varepsilon_4^{\perp}/G^{\perp} \cong \mathbb{Z}/4\mathbb{Z}$ is non-trivial, for otherwise we would have $\Gamma/G^{\perp} \cong G$, contrary to the fact that G is not Cogalois. Thus, $\Gamma/G^{\perp} \cong \varepsilon_4^{\perp}/G^{\perp} \rtimes \Gamma/\varepsilon_4^{\perp} \cong \mathbb{D}_8$, i.e., the action of $\Gamma/G^{\perp}$ on μ_G is of type D_8, as desired.

Case (ii): $p \in \mathbb{P} \setminus \{2\}$. We are going to show that $G^{\perp} \lhd \Gamma$ and the action of $\Gamma/G^{\perp}$ on μ_G is of type D_{pr}, where $r := (\Gamma : \varepsilon_p^{\perp})$. Let G' denote the subgroup of G consisting of all its elements of order prime to p. As G is Kneser, so is also G', and hence $(G'^{\perp} : G^{\perp}) = (G : G')$ is a power of the prime number p. Consequently, its divisor $(G'^{\perp} : G'^{\perp} \cap \varepsilon_p^{\perp})$ is also a power of p. On the other hand, as $\varepsilon_p^{\perp}$, the kernel of the non-trivial action of Γ on $A[p]$, is normal in Γ, we have $G'^{\perp} \cap \varepsilon_p^{\perp} \lhd G'^{\perp}$. So, the factor group $G'^{\perp}/G'^{\perp} \cap \varepsilon_p^{\perp}$ is identified with a subgroup of the cyclic group $\Gamma/\varepsilon_p^{\perp}$ of order r, with $r \,|\, p-1$ and $(r,p) = 1$. Therefore $G'^{\perp} \leqslant \varepsilon_p^{\perp}$. Since $G' \neq G$, it follows from the minimality of G that G' is Cogalois. Thus, $K := G' \cap \varepsilon_p^{\perp\perp}$ is also Cogalois and $K^{\perp} = \varepsilon_p^{\perp}$. Moreover, K is cyclic of order r since $\Gamma/K^{\perp} \cong \mathbb{Z}/r\mathbb{Z}$. In particular, we have $\mu_K = (1/r)\mathbb{Z}/\mathbb{Z} \leqslant A$. As $K^{\perp} \lhd \Gamma$, Corollaries 2.12 and 2.13 imply that $(1/r)\mathbb{Z}/\mathbb{Z} \leqslant A^{\varepsilon_p^{\perp}}$ and $K \cong Z^1(\Gamma/\varepsilon_p^{\perp}, (1/r)\mathbb{Z}/\mathbb{Z})$.

From the minimality condition satisfied by G it follows that $G = H \oplus K \cong \mathbb{Z}/pr\mathbb{Z}$ and $\mu_G = (1/pr)\mathbb{Z}/\mathbb{Z}$. Since $K^{\perp} = \varepsilon_p^{\perp} \lhd \Gamma$ and $((\Gamma : H^{\perp}), (\Gamma : K^{\perp})) = (p,r) = 1$, we deduce that $\Gamma = H^{\perp}K^{\perp}$ and $G^{\perp} = H^{\perp} \cap K^{\perp} \lhd H^{\perp}$. So, to conclude that $G^{\perp} \lhd \Gamma$ it suffices to show that $G^{\perp} \lhd K^{\perp}$. For any $\lambda \in G^{\perp}$, $\nu \in K^{\perp}$, $h \in H$ we have $h(\nu\lambda\nu^{-1}) = h(\nu) - (\nu\lambda\nu^{-1})h(\nu) = 0$ since $h(\nu) \in (1/p)\mathbb{Z}/\mathbb{Z} = A^{K^{\perp}}$ and $\nu\lambda\nu^{-1} \in K^{\perp}$. Thus $G^{\perp} \lhd \Gamma$, the kernel of the canonical action of $\Gamma/G^{\perp}$ on μ_G is $\varepsilon_4^{\perp}/G^{\perp}$, and $\Gamma/G^{\perp} = \varepsilon_4^{\perp}/G^{\perp} \rtimes H^{\perp}/G^{\perp}$. Let $\sigma \in H^{\perp}$, $\tau \in \varepsilon_p^{\perp}$, $u \in (\mathbb{Z}/pr\mathbb{Z})^*$ be such that $\sigma G^{\perp}$ is a generator of $H^{\perp}/G^{\perp} \cong \mathbb{Z}/r\mathbb{Z}$, $\tau G^{\perp}$ is a generator of $\varepsilon_p^{\perp}/G^{\perp} \cong \mathbb{Z}/p\mathbb{Z}$, and $\sigma\widehat{1/pr} = u\widehat{1/pr}$. Clearly $\tau\widehat{1/pr} = \widehat{1/pr}$ and the order of $u \bmod p \in (\mathbb{Z}/p\mathbb{Z})^*$ is r. Moreover, $\sigma\tau\sigma^{-1} \equiv \tau^u (\operatorname{mod} G^{\perp})$ since $G = H \oplus K$, $h(\sigma\tau\sigma^{-1}) = \sigma h(\tau) = uh(\tau) = h(\tau^u)$ for all $h \in H$ (as $h|_{\varepsilon_p^{\perp}} \in \operatorname{Hom}(\varepsilon_p^{\perp}, (1/p)\mathbb{Z}/\mathbb{Z})$), and $k(\sigma\tau\sigma^{-1}) = k(\tau^u) = 0$ for all $k \in K$.

Consequently, $\Gamma/G^{\perp} \cong \mathbb{Z}/p\mathbb{Z} \rtimes_u \mathbb{Z}/r\mathbb{Z}$. Therefore, to conclude that the action of $\Gamma/G^{\perp}$ on μ_G is of type D_{pr}, it remains only to check that $u \bmod l = 1 \bmod l$ i.e., $\widehat{1/l} \in A^{\Gamma}$ for all $l \in \mathcal{P}$, $l \,|\, r$. Assuming the contrary, let $l \in \mathcal{P}(\Gamma, A)$ be such that $l \,|\, r$. Since $\widehat{1/r} \in A^{\varepsilon_p^{\perp}}$, we deduce that $G^{\perp} \leqslant \varepsilon_p^{\perp} \leqslant \varepsilon_l^{\perp}$. Thus $l \in \mathcal{P}(\Gamma, A) \cap \mathcal{P}_G$ and $G^{\perp} \leqslant \varepsilon_l^{\perp}$, and hence $l \geqslant p$, which is a contradiction.

(2) $\Longrightarrow$ (1): Assume that $G^{\perp} \lhd \Gamma$ and the action of $\Gamma/G^{\perp}$ on μ_G is of one of the types D_4, D_8, or D_{pr}. Since G is canonically identified with a subgroup of $Z^1(\Gamma, \mu_G)$, we may assume without loss of generality that $G^{\perp} = \{1\}$ and $A = \mu_G$, i.e., (Γ, A) is one of the actions described in Definition 2.14. We have to show that every Kneser group $G \leqslant Z := Z^1(\Gamma, A)$ satisfying $G^{\perp} = \{1\}$ and $\mu_G = A$ is minimal non-Cogalois. We distinguish the following three cases:

Case (a): (Γ, A) is of type D_4. Then, the morphism $h \mapsto (h(\sigma), h(\tau))$ maps isomorphically Z onto $A \times 2A \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Thus $Z = \langle \varepsilon'_4 \rangle \oplus \langle \varphi \rangle$, where $\varphi \neq \varepsilon_4$ is defined by $\varphi(\sigma) = 0$, $\varphi(\tau) = \widehat{1/2}$. Notice that $G := \langle \varepsilon'_4 + \varphi \rangle \cong \mathbb{Z}/4\mathbb{Z}$ is the unique Kneser group of Z such that $\mu_G = A$, in particular $G^{\perp} = \{1\}$, and G is the unique Kneser non-Cogalois subgroup of Z as well.

Case (b): (Γ, A) is of type D_8. Then, the morphism $h \mapsto (h(\sigma), h(\tau))$ maps isomorphically Z onto $A \times A \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$. Consequently, $Z = \langle \varepsilon'_4 \rangle \oplus \langle \alpha \rangle$, where the cocycle α is defined by $\alpha(\sigma) = 0$, $\alpha(\tau) = \widehat{1/4}$. Observe that there exist only two Kneser groups G of Z such that $G^{\perp} = \{1\}$, i.e., $|G| = |\Gamma| = 8$, hence $\mu_G = A = (1/4)\mathbb{Z}/\mathbb{Z}$, namely $G_1 = \langle \varepsilon_4 \rangle \oplus \langle \alpha \rangle$ and $G_2 = \langle \varepsilon_4 \rangle \oplus \langle \alpha + \varepsilon'_4 \rangle$, both isomorphic to $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$ and stable under the action of Γ. They are also the only

Kneser (minimal) non-Cogalois groups of Z of order 8. Notice that, on the other hand, $\langle \varepsilon'_4 + 2\alpha\rangle \cong \mathbb{Z}/4\mathbb{Z}$ is the unique Kneser non-Cogalois subgroup of order 4, the corresponding action being of type D_4.

Case (c): (Γ, A) is of type D_{pr}, where p is an odd prime number and $r \mid p-1$, $r > 1$. Let $u \in (\mathbb{Z}/pr\mathbb{Z})^*$ be the unit defining the action. Since $N(\sigma) = \sum_{i=0}^{r-1} u^i = 0 \bmod pr$, the morphism $h \mapsto (h(\sigma), h(\tau))$ maps isomorphically Z onto $A \times rA \cong \mathbb{Z}/pr\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. Consequently, $Z = B_p \oplus \langle\alpha\rangle \oplus \langle\beta\rangle$, where the cocycles α and β are defined by $\alpha(\sigma) = \widehat{1/r}$, $\alpha(\tau) = 0$, $\beta(\sigma) = 0$, $\beta(\tau) = \widehat{1/p}$. As $\mathcal{P}(\Gamma, A) = \{p\}$, the necessary and sufficient condition for a subgroup G of Z to be Kneser is, according to Theorem 1.13, that $G \cap B_p = 0$. Consequently, G is a maximal Kneser group of Z if and only if G is a direct summand of B_p if and only if G is a Kneser group isomorphic to $\mathbb{Z}/pr\mathbb{Z}$ if and only if G is a Kneser group with $G^\perp = \{1\}$ if and only if G is a Kneser group with $\mu_G = A$. The only subgroups of Z satisfying the equivalent conditions above are the subgroups $G_i = \langle i\varepsilon_p + \alpha + \beta\rangle \cong \mathbb{Z}/pr\mathbb{Z}$, $i \in \mathbb{Z}/p\mathbb{Z}$. Since $\mathcal{P}(\Gamma, A) = \{p\}$ and the unique subgroup $H \leqslant G_i, i \in \mathbb{Z}/p\mathbb{Z}$, for which $p \mid |H|$ and $H^\perp \leqslant \varepsilon_p^\perp$ is the whole group G_i, it follows by Theorem 2.5 that the G_i's are also the only Kneser non-Cogalois subgroups of Z. Notice that, in contrast with the actions of type D_4 or D_8, the subgroups $G_i, i \in \mathbb{Z}/p\mathbb{Z}$ are not stable under the action of Γ. More precisely, Γ acts transitively on the set $\{\, G_i \mid i \in \mathbb{Z}/p\mathbb{Z}\}$ with stabilizers $\langle \tau^i \sigma \tau^{-i}\rangle \cong \mathbb{Z}/r\mathbb{Z}, i \in \mathbb{Z}/p\mathbb{Z}$. □

Corollary 2.16. *Any Kneser minimal non-Cogalois group of $Z^1(\Gamma, A)$ is isomorphic either to $\mathbb{Z}/4\mathbb{Z}$, or to $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$, or to $\mathbb{Z}/pr\mathbb{Z}$ for an odd prime number p and a divisor $r \neq 1$ of $p-1$.*

Proof. Let G be a Kneser minimal non-Cogalois group of $Z^1(\Gamma, A)$. By Lemma 2.15., $G^\perp \lhd \Gamma$ and the action of $\Gamma/G^\perp$ on μ_G is of one of the types $\mathrm{D}_4, \mathrm{D}_8$ or D_{pr}. The possible isomorphism types for the group G are now immediate from the proof of the implication (2) $\Longrightarrow$ (1) of Lemma 2.15. □

The next result provides an analogue of Theorem 1.13 for Cogalois groups.

Theorem 2.17. *The following statements are equivalent for a Kneser subgroup G of $Z^1(\Gamma, A)$.*

(1) *G is Cogalois.*

(2) *G contains no H for which $H^\perp \lhd \Gamma$ and the action of $\Gamma/H^\perp$ on μ_H is one of the types D_4, D_8, or D_{pr}.*

Proof. The result follows at once from Lemma 2.15 and from the following fact we already mentioned just before Lemma 2.15: for any $L \in \mathcal{M}(\Gamma, A)$ there exists at least one $K \in \mathcal{M}(\Gamma, A)_{\min}$ such that $K \subseteq L$. □

As it follows from Lemma 2.15, the fact that all the p-primary components of a subgroup G of $Z^1(\Gamma, A)$ are Cogalois does not imply that the whole group G is Cogalois. The next result provides a supplementary lattice theoretic condition which ensures such an implication, obtaining in this way a *local-global principle* for Cogalois groups.

Theorem 2.18. *Let G be a subgroup of $Z^1(\Gamma, A)$, and let*

$$\theta : \overline{\mathbb{L}}(\Gamma|G^{\perp}) \longrightarrow \prod_{p\in\mathbb{P}} \overline{\mathbb{L}}(\Gamma|G(p)^{\perp}),\ \Delta \mapsto (\overline{\langle \Delta \cup G(p)^{\perp}\rangle})_{p\in\mathbb{P}}.$$

Then, the following statements are equivalent.

(1) *G is Cogalois.*

(2) *$G(p)$ is Cogalois for all prime numbers p, and the order-preserving map θ is a lattice isomorphism.*

(3) *G is Kneser, $G(2)$ is Cogalois, and $\Delta = \Gamma$ whenever $\Delta \in \overline{\mathbb{L}}(\Gamma|G^{\perp})$ is such that $\theta(\Delta) = \theta(\Gamma)$.*

Proof. (1) $\Longrightarrow$ (2): Assuming that G is Cogalois, we only have to prove that θ is a lattice isomorphism. As G and the $G(p)$'s are Cogalois, the canonical order-reversing maps $\varphi : \mathbb{L}(G) \longrightarrow \overline{\mathbb{L}}(\Gamma|G^{\perp})$, $\varphi_p : \mathbb{L}(G(p)) \longrightarrow \overline{\mathbb{L}}(\Gamma|G(p)^{\perp})$, $H \mapsto H^{\perp}$ are lattice anti-isomorphisms. On the other hand, since the canonical map

$$\psi : \mathbb{L}(G) \longrightarrow \prod_{p\in\mathbb{P}} \mathbb{L}(G(p)),\ H \mapsto (H(p))_{p\in\mathbb{P}}$$

is a lattice isomorphism, the composed map

$$(\prod_{p\in\mathbb{P}} \varphi_p) \circ \psi \circ \varphi^{-1} : \overline{\mathbb{L}}(\Gamma|G^{\perp}) \longrightarrow \prod_{p\in\mathbb{P}} \overline{\mathbb{L}}(\Gamma|G(p)^{\perp}),\ \Delta \mapsto ((G \cap \Delta^{\perp})(p)^{\perp})_{p\in\mathbb{P}}$$

is also a lattice isomorphism, so it remains only to check that $(\prod_{p\in\mathbb{P}} \varphi_p) \circ \psi \circ \varphi^{-1} = \theta$, i.e., $(G \cap \Delta^{\perp})(p)^{\perp} = \overline{\langle \Delta \cup G(p)^{\perp}\rangle}$ for all $p \in \mathbb{P}, \Delta \in \overline{\mathbb{L}}(\Gamma|G^{\perp})$. Now, as φ is a lattice anti-isomorphism, we deduce that

$$(G \cap \Delta^{\perp})(p)^{\perp} = ((G \cap \Delta^{\perp}) \cap G(p))^{\perp} = \overline{\langle (G \cap \Delta^{\perp})^{\perp} \cup G(p)^{\perp}\rangle} = \overline{\langle \Delta \cup G(p)^{\perp}\rangle},$$

as desired.

(2) $\Longrightarrow$ (3) follows at once from Corollary 1.11.

(3) $\Longrightarrow$ (1): Assuming that G is Kneser but not Cogalois, we have to show that either $G(2)$ is not Cogalois or there exists $\Delta \in \overline{\mathbb{L}}(\Gamma|G^{\perp})$ such that $\Delta \neq \Gamma$ and $\theta(\Delta) = \theta(\Gamma)$. Let H be a minimal non-Cogalois subgroup of G. According to Lemma 2.15, $H^{\perp}$ is an open normal subgroup of Γ and the action of $\Gamma/H^{\perp}$ on μ_H is one of the actions described in Definition 2.14. If the action above is of type D_4 or of type D_8, then it follows that $H \leqslant G(2)$, and hence $G(2)$ is not Cogalois. So, it remains to consider only the case when the action is of type D_{pr}, where p is an odd prime number and $r \,|\, p-1$, $r \geqslant 2$. Notice that $\overline{\langle H^{\perp} \cup G(p)^{\perp}\rangle} = H^{\perp}G(p)^{\perp}$ as $H^{\perp} \lhd \Gamma$, $(\Gamma : H^{\perp}G(p)^{\perp})$ is a power of p as $G \in \mathcal{K}(\Gamma, A)$, and $(\Gamma : H(p)^{\perp}) = |H(p)| = p$ as $H(p) \leqslant G \in \mathcal{K}(\Gamma, A)$

and $H(p) \cong \mathbb{Z}/p\mathbb{Z}$ (since $H \cong \mathbb{Z}/pr\mathbb{Z}$ by Corollary 2.16 and $(p,r)=1$). On the other hand, since $H^\perp \leqslant H^\perp G(p)^\perp \leqslant H(p)^\perp \leqslant \Gamma$ and $(\Gamma : H^\perp) = pr$, $r \,|\, p-1$, it follows that $H^\perp G(p)^\perp = H(p)^\perp$. As $\Gamma/H^\perp \cong \mathbb{Z}/p\mathbb{Z} \rtimes_u \mathbb{Z}/r\mathbb{Z}$ for a suitable $u \in (\mathbb{Z}/pr\mathbb{Z})^*$ by Definition 2.14, there exists an open subgroup Δ of Γ lying over $H^\perp$ such that $(\Gamma : \Delta) = p$ and $\Delta \neq H(p)^\perp$. Consequently, $\overline{\langle \Delta \cup G(p)^\perp \rangle} = \overline{\langle \Delta \cup H(p)^\perp \rangle} = \Gamma$, and, similarly, $\overline{\langle \Delta \cup G(q)^\perp \rangle} = \Gamma$ for any prime number $q \neq p$ since all open subgroups of Γ lying over $G(q)^\perp$ have q-th power indices in Γ as $G \in \mathcal{K}(\Gamma, A)$. Thus, we found a subgroup Δ of Γ with the desired properties, which finishes the proof. $\square$

Finally, we consider the case when G is stable under the action of Γ. Then, the local-global principle for Cogalois groups has the following simple formulation.

Proposition 2.19. *The following assertions are equivalent for a Γ-submodule G of $Z^1(\Gamma, A)$.*

(1) *G is Cogalois.*

(2) *$G(p)$ is Cogalois for all prime numbers p.*

(3) *G is Kneser, and $G(2)$ is Cogalois.*

Proof. The implication (1) $\Longrightarrow$ (2) is trivial, while the implication (2) $\Longrightarrow$ (3) follows at once from Corollary 1.11.

(3) $\Longrightarrow$ (1): Assuming that the Γ-module G is Kneser but not Cogalois, we have only to show that $G(2)$ is not Cogalois. Let H be a minimal non-Cogalois subgroup of G. According to Lemma 2.15, $H^\perp \lhd \Gamma$ and the action of $\Gamma/H^\perp$ on μ_H is the one described in Definition 2.14. If the action is of type D_4 or of type D_8, then $H \leqslant G(2)$, and hence $G(2)$ is not Cogalois, as desired. Now assume that the action is of type D_{pr}. Then, as in the proof of Theorem 2.18 we deduce that $(\Gamma : H^\perp G(p)^\perp) = p$. On the other hand, $G(p)^\perp \lhd \Gamma$ since $G(p)$ is a Γ-submodule of G. Hence $H^\perp G(p)^\perp \lhd \Gamma$, and so, $\mathbb{Z}/p\mathbb{Z}$ is a quotient of $\Gamma/H^\perp \cong \mathbb{Z}/p\mathbb{Z} \rtimes_u \mathbb{Z}/r\mathbb{Z}$, which is a contradiction. $\square$

References

[1] T. ALBU, *Infinite field extensions with Cogalois correspondence*, Comm. Algebra **30** (2002), 2335-2353.

[2] T. ALBU, "*Cogalois Theory*", A Series of Monographs and Textbooks, Vol. 252, Marcel Dekker, Inc., New York and Basel, 2002, 368 pp.

[3] T. ALBU, *Infinite field extensions with Galois-Cogalois correspondence (I)*, Rev. Roumaine Mat. Pures Appl. **47** (2002), to appear.

[4] T. ALBU, *Infinite field extensions with Galois-Cogalois correspondence (II)*, Rev. Roumaine Mat. Pures Appl. **47** (2002), to appear.

[5] T. ALBU and Ş. BASARAB, *Lattice-isomorphic groups, and infinite Abelian G-Cogalois field extensions*, J. Algebra Appl. **1** (2002), 243-253.

[6] T. ALBU and F. NICOLAE, *Kneser field extensions with Cogalois correspondence*, J. Number Theory **52** (1995), 299-318.

[7] T. ALBU and F. NICOLAE, *Finite radical field extensions and crossed homomorphisms*, J. Number Theory **60** (1996), 291-309.

[8] T. ALBU and M. ŢENA, *Infinite Cogalois Theory*, Mathematical Reports **3 (53)** (2001), 105-132.

[9] G. KARPILOVSKY, "*Topics in Field Theory*", North-Holland, Amsterdam, 1989.

[10] M. KNESER, *Lineare Abhängigkeit von Wurzeln*, Acta Arith. **26** (1975), 307-308.

[11] J. NEUKIRCH, "*Algebraische Zahlentheorie.*" Springer-Verlag, Berlin Heidelberg New York, 1992.

[12] J.P. SERRE, "*Cohomologie Galoisienne*", Lecture Notes in Mathematics **5**, Springer-Verlag, Berlin, 1964.

[13] B. STENSTRÖM, "*Rings of Quotients*", Springer-Verlag, Berlin, Heidelberg, and New York, 1975.