JOURNAL DE THÉORIE DES NOMBRES DE BORDEAUX

K. W. GRUENBERG

A. WEISS

Capitulation and transfer kernels

Journal de Théorie des Nombres de Bordeaux, tome 12, nº 1 (2000), p. 219-226

<http://www.numdam.org/item?id=JTNB_2000__12_1_219_0>

Journal de Théorie des Nombres
de Bordeaux **12** (2000), 219–226

Capitulation and Transfer Kernels

par K. W. GRUENBERG et A. WEISS

RÉSUMÉ. On sait que pour une extension galoisienne finie K/k d'un corps de nombres, le noyau du morphisme d'extension $\mathrm{Cl}_k \to \mathrm{Cl}_K$ s'identifie au noyau $X(H)$ du transfert $H/H' \to A$, où $H = \mathrm{Gal}(\tilde{K}/k)$, $A = \mathrm{Gal}(\tilde{K}/K)$ et $\tilde{K}$ est le corps de classes de Hilbert de K. Lorsque le groupe $G = \mathrm{Gal}(K/k)$ est abélien, H. Suzuki a montré que $|G|$ divise $|X(H)|$.

Nous appelons noyau de transfert pour G tout groupe abélien fini X qui s'écrit $X(H)$ pour un certain groupe H tel que $A \hookrightarrow H \twoheadrightarrow G$. Après avoir caractérisé les noyaux de transfert en termes de représentations entières de G, nous montrons que X est un noyau de transfert pour le groupe abélien G si et seulement si on a $|G|X = 0$ et $|G|$ divise $|X|$, ce qui fournit une nouvelle démonstration du résultat de Suzuki.

ABSTRACT. If K/k is a finite Galois extension of number fields with Galois group G, then the kernel of the capitulation map $\mathrm{Cl}_k \to \mathrm{Cl}_K$ of ideal class groups is isomorphic to the kernel $X(H)$ of the transfer map $H/H' \to A$, where $H = \mathrm{Gal}(\tilde{K}/k)$, $A = \mathrm{Gal}(\tilde{K}/K)$ and $\tilde{K}$ is the Hilbert class field of K. H. Suzuki proved that when G is abelian, $|G|$ divides $|X(H)|$. We call a finite abelian group X a transfer kernel for G if $X \cong X(H)$ for some group extension $A \hookrightarrow H \twoheadrightarrow G$.

After characterizing transfer kernels in terms of integral representations of G, we show that X is a transfer kernel for the abelian group G if and only if $|G|X = 0$ and $|G|$ divides $|X|$. Our arguments give a new proof of Suzuki's result.

Let K/k be a finite unramified Galois extension of number fields with Galois group G. The capitulation kernel for K/k is the kernel of the natural homomorphism of ideal class groups $\mathrm{Cl}_k \to \mathrm{Cl}_K$. Suzuki [S] proved that when G is abelian, its order $|G|$ divides the order of the capitulation kernel. This remarkable result encapsulates much of the information previously available about capitulation. We refer to the surveys [J] and [M]

Manuscrit reçu le 23 septembre 1999.
The authors gratefully acknowledge financial help from EPSRC and NSERC.

for relevant background. Our aim here is to explain a new approach to Suzuki's theorem.

The transition to group theory (reviewed in § 1) allows one to interpret capitulation kernels as transfer kernels, by which we mean the following: given a finite group G, then a finite abelian group X is a *transfer kernel for* G if there exists a group extension $A \hookrightarrow H \twoheadrightarrow G$ with A finite abelian so that X is isomorphic to the kernel of the transfer homomorphism $H/[H,H] \to A$. We shall prove the following result.

Theorem 1. *If G is a finite abelian group, then the finite additive group X is a transfer kernel for G if, and only if, $|G|X = 0$ and $|G|$ divides $|X|$.*

We outline what follows. In §1 we translate the problem into an equivalent one on G-module extensions over ΔG, the augmentation ideal of the integral group ring $\mathbb{Z}G$. Then §2, the core of the paper, is an analysis of the common structural properties of transfer kernels for G. This makes possible the proof of Theorem 1 in §3. In our final §4 we collect some comments and questions.

1. Translations

We begin with the classical result of E. Artin.

Proposition 1. *The capitulation kernel for K/k is a transfer kernel for G.*

Here is a sketch of the proof. Let $\widetilde{K}$ be the Hilbert class field of K and $A = \mathrm{Gal}(\widetilde{K}/K)$. If $H = \mathrm{Gal}(\widetilde{K}/k)$ then there is a commutative square

$$\begin{array}{ccc} \mathrm{Cl}_k & \xrightarrow{\simeq} & H/[H,H] \\ {\scriptstyle \text{capitulation}}\downarrow & & \downarrow{\scriptstyle \text{transfer}} \\ \mathrm{Cl}_K & \xrightarrow{\simeq} & A \end{array}$$

from which the proposition follows by taking kernels.

Proposition 2. *The finite additive group X is a transfer kernel for G if, and only if, there exists a G-module extension $A \rightarrowtail B \twoheadrightarrow \Delta G$ with A finite and $X \simeq \mathrm{H}^{-1}(G,B)$.*

Proof. This result is clear from the functorial relationship between group extensions over G and G-module extensions over ΔG (cf. [G] §10.5). As this is not the usual approach in the literature we sketch it here.

A group extension

$$A \overset{i}{\rightarrowtail} H \overset{\pi}{\twoheadrightarrow} G \tag{1}$$

yields the G-module extension

$$(2) \qquad A \overset{j}{\rightarrowtail} B \overset{\tau}{\twoheadrightarrow} \Delta G$$

where $B = \Delta H/\Delta A.\Delta H$, τ is induced from $\pi : \Delta H \to \Delta G$ and $j(a)$ is the appropriate coset of $i(a) - 1$.

Conversely, given (2), let

$$\widetilde{H} = \{b \in B \mid \tau(b) = g - 1, \text{ for some } g \in G\}.$$

Then $\widetilde{H}$ is a group with multiplication $x.y = \tau(x)y + x + y$, its identity element is 0 and the inverse of x is $x^{-1} = -g^{-1}x$, where $\tau(x) = g - 1$. The module homomorphism τ gives the group homomorphism $\widetilde{H} \twoheadrightarrow G$ via $x \mapsto \tau(x) + 1$ with kernel A.

If B arises from the group extension (1), then the *hidden group* $\widetilde{H}$ in B gives an extension equivalent to H:

$$(3) \qquad \begin{array}{ccccc} & & H & & \\ & \nearrow & & \searrow & \\ A & & \Big\downarrow \sigma & & G \\ & \searrow & & \nearrow & \\ & & \widetilde{H} & & \end{array}$$

where $\sigma(h) = (h - 1) + \Delta A.\Delta H$. The G-coinvariants on B, namely $B_G = B/(\Delta G)B$, are naturally isomorphic to $\Delta H/(\Delta H)^2$, whence to $H/[H, H]$ and so to $\widetilde{H}/[\widetilde{H}, \widetilde{H}]$. Notice that $\widetilde{H}/[\widetilde{H}, \widetilde{H}] \cong B_G$ is just $x[\widetilde{H}, \widetilde{H}] \mapsto x + (\Delta G)B$.

We claim there is a commutative square

$$\begin{array}{ccc} H/[H,H] & \xrightarrow{\simeq} & B_G \\ \text{transfer}\Big\downarrow & & \Big\downarrow \widehat{G} \\ A^G & \xrightarrow{\simeq} & B^G \end{array}$$

where $\widehat{G}$ is the norm endomorphism $\Sigma_{g \in G}\, g$ and the lower isomorphism is induced by j.

In view of (3) we may replace H by $\widetilde{H}$ and view j as inclusion. Take a transversal t_g, $g \in G$, for A in $\widetilde{H}$. If $x \in \widetilde{H}$ with $\tau(x) = k - 1$, then the image of x under transfer is $\Pi_g\, t_{kg}^{-1}.x.t_g$, which is the same as $\Sigma_g\, t_{kg}^{-1}.x.t_g$, because each factor is in A. Now

$$\begin{aligned} t_{kg}^{-1}.x.t_g &= (-(kg)^{-1}t_{kg}).(kt_g + x) \\ &= (kg)^{-1}(kt_g + x) - (kg)^{-1}t_{kg} \\ &= g^{-1}t_g + (kg)^{-1}x - (kg)^{-1}t_{kg} \end{aligned}$$

and so the transfer image is $\widehat{G}x$ as required.

Proposition 2 follows by taking kernels. □

2. Transfer kernels

Let G be a finite group, not necessarily abelian. Put $\Lambda = \mathbb{Z}G/(\widehat{G})$ and identify Λ_G with $\mathbb{Z}/|G|\mathbb{Z}$. If M is a $\mathbb{Z}G$-module, then $d_G(M)$ denotes the minimum number of module generators of M.

Theorem 2. *The following are equivalent:*

(a) *X is a transfer kernel for G;*

(b) *X is isomorphic to the cokernel of a homomorphism $\varphi : U_G \to \Lambda_G^m$, where $m \geq d_G(\Delta G)$ and U is a finitely generated G-submodule of $\mathbb{Q}\Lambda^{m-1}$;*

(c) *X is isomorphic to M_G for some finitely generated G-module M, where $\widehat{G}M = 0$ and $\mathbb{Q}M$ contains a $\mathbb{Q}G$-copy of $\mathbb{Q}\Lambda$;*

(d) *$|G|X = 0$ and there exists a surjective homomorphism $X \twoheadrightarrow M_G$ with M as in* **(c)**.

Proof. **(a)** ⇒ **(b)**. Using Proposition 2 we may, and shall, assume $X \simeq \mathrm{H}^{-1}(G,B)$, where $A \rightarrowtail B \twoheadrightarrow \Delta G$. Take a free resolution of B, so determining m and S in the following diagram:

$$\begin{array}{ccccc} S & \xrightarrow{=} & S & & \\ \downarrow & & \downarrow & & \\ R & \rightarrowtail & \mathbb{Z}G^m & \twoheadrightarrow & \Delta G \\ \downarrow & & \downarrow & & \downarrow \| \\ A & \rightarrowtail & B & \twoheadrightarrow & \Delta G \end{array} \tag{4}$$

Now $\mathrm{H}^{-1}(G,B) \simeq \mathrm{H}^0(G,S)$ (we use Tate cohomology throughout) and the exact sequence $S^G \hookrightarrow S \twoheadrightarrow U$ gives

$$\mathrm{H}^{-1}(G,U) \xrightarrow{\delta} \mathrm{H}^0(G,S^G) \longrightarrow \mathrm{H}^0(G,S),$$

where δ is the connecting homomorphism. Since A is finite, $\mathbb{Q}S = \mathbb{Q}R \simeq \mathbb{Q} \oplus \mathbb{Q}G^{m-1}$, whence $S^G \simeq \mathbb{Z}^m$ and $\mathbb{Q}U \simeq \mathbb{Q}\Lambda^{m-1}$. Note that U is $\mathbb{Z}$-torsion-free and so U is contained in $\mathbb{Q}U$. Also $\widehat{G}U = 0$ gives $\mathrm{H}^{-1}(G,U) = U_G$ and $\mathrm{H}^0(G,U) = 0$. Thus $U_G \xrightarrow{\delta} \Lambda_G^m \twoheadrightarrow X$ is exact.

(b) ⇒ **(c)**. The exact sequence $\Delta G \rightarrowtail \Lambda \twoheadrightarrow \Lambda_G$ of G-modules stays exact when we apply $\mathrm{Hom}(U,-)$ because U is $\mathbb{Z}$-free. So we obtain the exact sequence

$$\mathrm{Hom}_G(U,\Lambda^m) \longrightarrow \mathrm{Hom}(U_G,\Lambda_G^m) \longrightarrow \mathrm{H}^1(G,\mathrm{Hom}(U,\Delta G^m)),$$

where the right hand term is 0 because it is isomorphic to $\mathrm{H}^0(G,\mathrm{Hom}(U,\mathbb{Z}^m))$, which is 0 because $\mathrm{Hom}_G(U,\mathbb{Z}) = 0$ as U_G is finite.

It follows that the given homomorphism $\varphi : U_G \to \Lambda_G^m$ lifts to a G-homomorphism $\beta : U \to \Lambda^m$ with $\beta_G = \varphi$ giving the commutative diagram

$$\begin{array}{ccccc} U & \xrightarrow{\beta} & \Lambda^m & \twoheadrightarrow & M \\ \downarrow & & \downarrow & & \\ U_G & \xrightarrow{\varphi} & \Lambda_G^m & \twoheadrightarrow & X \end{array}$$

with $M = \mathrm{Coker}\beta$. This induces an epimorphism $M \twoheadrightarrow X$ and hence, by taking G-coinvariants, an isomorphism $M_G \simeq X$. Finally, $\mathbb{Q}M \oplus \mathbb{Q}U$ contains (a G-copy of) $\mathbb{Q}\Lambda^m$, whence $\mathbb{Q}M$ contains $\mathbb{Q}\Lambda$.

(c) $\Rightarrow$ **(d)** is clear since $|G|$ annihilates $M_G = \mathrm{H}^{-1}(G, M)$.

(d) $\Rightarrow$ **(b)**. Choose $m \geq \max\{d_G(M),\ d_G(\Delta G),\ d(X)\}$ and take a G-free presentation $L \hookrightarrow \mathbb{Z}G^m \twoheadrightarrow M$ of M. Since $\widehat{G}M = 0$, $L^G = (\mathbb{Z}G^m)^G$, thereby giving the exact sequence $U \overset{i}{\hookrightarrow} \Lambda^m \twoheadrightarrow M$, where $U = L/L^G$, and hence the exact sequence $U_G \xrightarrow{i_G} \Lambda_G^m \twoheadrightarrow M_G$. Choose $\alpha : \Lambda_G^m \twoheadrightarrow X$ and let $\beta : X \twoheadrightarrow M_G$ be the given homomorphism. Thus $\mathrm{Coker}\, i_G \simeq M_G \simeq \mathrm{Im}\beta\alpha$, which implies, by the Lemma below, that $\mathrm{Im}\, i_G \simeq \mathrm{Ker}\beta\alpha$. Consequently $\mathrm{Ker}\alpha$ is isomorphic to a subgroup D of $\mathrm{Im}\, i_G$. There exists a map of U_G onto D (remember we are dealing with finite abelian groups), giving the composite $\varphi : U_G \twoheadrightarrow D \hookrightarrow \Lambda_G^m$, with $\mathrm{Im}\varphi \simeq \mathrm{Ker}\alpha$. Again using the Lemma below, $\mathrm{Coker}\varphi \simeq \mathrm{Im}\alpha \simeq X$ and so $U_G \xrightarrow{\varphi} \Lambda_G^m \twoheadrightarrow X$ is exact. Finally, $\mathbb{Q}U \oplus \mathbb{Q}M \simeq \mathbb{Q}\Lambda^m$ shows that $\mathbb{Q}M \supseteq \mathbb{Q}\Lambda$ implies $\mathbb{Q}U \subseteq \mathbb{Q}\Lambda^{m-1}$.

Lemma. (i) *Given epimorphisms* $f_1, f_2 : \Lambda_G^m \twoheadrightarrow X$, *then* $\mathrm{Ker}f_1 \simeq \mathrm{Ker}f_2$.
(ii) *Given epimorphisms* $g_i : \Lambda_G^m \twoheadrightarrow X_i$, $i = 1, 2$, *with* $\mathrm{Ker}g_1 \simeq \mathrm{Ker}g_2$, *then* $X_1 \simeq X_2$.

Proof. In (i) the homomorphisms f_1, f_2 are free presentations of X as $\mathbb{Z}/|G|\mathbb{Z}$-module. So Schanuel's Lemma and the Krull-Schmidt property give the result. For (ii), dualise with respect to $\mathbb{Q}/\mathbb{Z}$ and obtain $X_1^* \simeq X_2^*$ by (i).

(b) $\Rightarrow$ **(a)**. Our aim is to prove that the X of (b) is a transfer kernel in the module-theoretic sense of Proposition 2.

We use the isomorphism

$$\mathrm{H}^1(G, \mathrm{Hom}(U, \mathbb{Z}^m)) \simeq \mathrm{Hom}(\mathrm{H}^{-1}(G, U),\ \mathrm{H}^0(G, \mathbb{Z}^m))$$

given by integral duality: $\xi \mapsto (x \mapsto \xi.x)$. Hence φ corresponds to a uniquely determined extension $\mathbb{Z}^m \rightarrowtail S \twoheadrightarrow U$ whose associated connecting homomorphism $\mathrm{H}^{-1}(G, U) \to \mathrm{H}^0(G, \mathbb{Z}^m)$ is φ (e.g. 11.1 in [GW]). Thus $U_G \xrightarrow{\varphi} \Lambda_G^m \twoheadrightarrow \mathrm{H}^0(G, S)$ is exact and so $X \simeq \mathrm{H}^0(G, S)$.

Take a free presentation $R \hookrightarrow \mathbb{Z}G^m \twoheadrightarrow \Delta G$ of ΔG and embed S in R with cokernel A. This can be done because

$$\mathbb{Q}S \simeq \mathbb{Q}^m \oplus \mathbb{Q}U \subseteq \mathbb{Q}^m \oplus \mathbb{Q}\Lambda^{m-1} \simeq \mathbb{Q} \oplus \mathbb{Q}G^{m-1} \simeq \mathbb{Q}R.$$

Taking the pushout along $R \twoheadrightarrow A$ gives a diagram exactly like (4) except that A might not be finite. In any case $\mathrm{H}^0(G,S) \simeq \mathrm{H}^{-1}(G,B)$.

It remains to find a submodule L of A so that A/L is finite and $\mathrm{H}^{-1}(G,B) \simeq H^{-1}(G,B/L)$. First note that $\mathbb{Q}B^G = 0$ by the middle column of (4) and $\mathbb{Q}S^G \simeq \mathbb{Q}^m$. Hence B_G is finite and so $A/A \cap \Delta G.B$ is finite. Pick a torsion-free G-submodule L of finite index in $A \cap \Delta G.B$. Then A/L is finite; also $\widehat{G}L = 0$, whence $L^G = 0$. The exact sequence $L \hookrightarrow B \twoheadrightarrow B/L$ then gives the exact sequence

$$\mathrm{H}^{-1}(G,L) \xrightarrow{0} \mathrm{H}^{-1}(G,B) \longrightarrow \mathrm{H}^{-1}(G,B/L) \longrightarrow \mathrm{H}^0(G,L) = 0,$$

which finishes the proof. □

3. Proof of Theorem 1

To prove Theorem 1 it suffices, in view of Proposition 2 and Theorem 2, to establish the equivalence of

(i) *X is a finite additive group such that* $|G|X = 0$ *and* $|G|$ *divides* $|X|$;

with

(ii) *X is isomorphic to M_G for some finitely generated G-module M, where $\widehat{G}M = 0$ and $\mathbb{Q}M$ contains a $\mathbb{Q}G$-copy of $\mathbb{Q}\Lambda$.*

(i) ⇒ (ii). By (d) of Theorem 2 it suffices to prove X has a transfer kernel for G as a homomorphic image. We shall show that any image of X of order $|G|$ is a transfer kernel. Change notation and call this image X. So we have $|X| = |G|$ and shall use induction on $|X|$: when $X = 0$, then $G = 1$ and so we can take $M = 0$.

Now let $X = X_1 \oplus \mathbb{Z}/p^s\mathbb{Z}$. Since $|G| = |X|$, so G has an image $\overline{G} = G/G_1$ of order p^s and then $|G_1| = |X_1|$. By induction, $X_1 \simeq (M_1)_{G_1}$ for an appropriate M_1. Define $M = \mathrm{Ind}_{G_1}^G(M_1) \oplus \bar{\Lambda}$, where $\bar{\Lambda} = \mathbb{Z}\overline{G}/(\widehat{\overline{G}})$ is a G-module by inflation. Then $\widehat{G}M = 0$ since $\widehat{G}_1 M_1 = 0$, whence

$$\begin{aligned} M_G = \mathrm{H}^{-1}(G,M) &= \mathrm{H}^{-1}(G_1,M_1) \oplus \mathrm{H}^{-1}(G,\bar{\Lambda}) \\ &= (M_1)_{G_1} \oplus \bar{\Lambda}_G = X_1 \oplus \bar{\Lambda}_{\bar{G}} = X. \end{aligned}$$

Also, since $\mathbb{Q}M_1 \supseteq \mathbb{Q}\Lambda_1$ so $\mathbb{Q}M \supseteq \mathbb{Q}(\mathrm{Ind}_{G_1}^G \Lambda_1) \oplus \mathbb{Q}\bar{\Lambda} \simeq \mathbb{Q}\Lambda$, as required.

(ii) ⇒ (i). We repeat the classical argument. Take a free $\mathbb{Z}G$-presentation $F \twoheadrightarrow M$ of M, with $F = \mathbb{Z}G^m$. Since M_G is finite, the kernel of $F_G \twoheadrightarrow M_G$ is isomorphic to F_G and so M_G is the cokernel of an endomorphism f of F_G. It follows that $\det f = \pm|M_G|$.

Since $F \to F_G$ maps $\mathrm{Ker}(F \to M)$ onto the image of f, there is a $\mathbb{Z}G$-endomorphism $\tilde{f}$ of F such that $\tilde{f}_G = f$ and $\mathrm{Coker}\tilde{f}$ maps onto M. Now $\det \tilde{f}$ annihilates $\mathrm{Coker}\tilde{f}$ (recall that $\mathbb{Z}G$ is a commutative ring). So

$(\det \tilde{f})M = 0$ implies $\det \tilde{f} = n\widehat{G}$ for a suitable integer n (since $\mathbb{Q}\Lambda \subseteq \mathbb{Q}M$).

Finally, with ε denoting the augmentation on $\mathbb{Z}G$, $\varepsilon \det \tilde{f} = \det f$ and thus $n|G| = \varepsilon(n\widehat{G}) = \pm|M_G|$.

4. Remarks

(1) Is the converse of Proposition 1 true? This is a fundamental problem. An even stronger form of this is the following: given a group extension $A \to H \to G$ with A abelian, does there exist an unramified Galois extension L with Galois group H so that L is the Hilbert class field $\widetilde{K}$ of the fixed field K of A?

It should be noticed that any group H can be realised as the Galois group of an unramified extension L/k ([L], p. 121). Then $L \subseteq \widetilde{K}$ and the difficulty lies in ensuring that $L = \widetilde{K}$.

(2) Suppose X is a finite additive group such that $|G|X = 0$. Then

(a) if X is a transfer kernel for G, $|G/[G,G]|$ divides $|X|$;

(b) if $|G|$ divides $|X|$, then X is a transfer kernel for G.

Both these facts are variations of §3; for (b) one must first show that if, for each prime p, the p-primary part of X is a transfer kernel for a Sylow p-subgroup of G, then X is one for G.

However, neither (a) nor (b) has a converse if G is a non-abelian p-group. This is obvious for (b) (take $A = 1$). For (a), if X is $\mathbb{Z}$-cyclic and of order $|G/[G,G]|$, then X cannot be a transfer kernel for G: for if $X \simeq M_G$ with M as in (c) of Theorem 2, then lifting a generator of M_G to M gives a G-homomorphism $\Lambda \to M$ which becomes an isomorphism on coinvariants (by Nakayama's Lemma and $\mathbb{Q}M \supseteq \mathbb{Q}\Lambda$); then $|X| = |G|$ forcing G to be abelian.

References

[G] K.W. Gruenberg, *Relation Modules of Finite Groups.* CBMS Monograph 25, Amer. Math. Soc., Providence, R.I., 1976.

[GW] K.W. Gruenberg, A. Weiss, *Galois invariants for units.* Proc. London Math. Soc. **70** (1995), 264–284.

[J] J.-F. Jaulent, *L'état actuel du problème de la capitulation.* Sem. de Théorie des Nombres de Bordeaux, 1987-1988, exposé no.17.

[L] S. Lang, *Algebraic Number Theory.* Springer, New York, 1994.

[M] K. Miyake, *Algebraic investigations of Hilbert's Theorem 94, the principal ideal theorem and the capitulation problem.* Expo. Math. **7** (1989), 289–346.

[S] H. Suzuki, *A generalization of Hilbert's Theorem 94.* Nagoya Math. J. **121** (1991), 161–169.

K. W. GRUENBERG
School of Mathematical Sciences
Queen Mary and Westfield College
Mile End Road
London E1 4NS, England
E-mail : K.W.Gruenberg@qmw.ac.uk

A. WEISS
Department of Mathematics
University of Alberta
Edmonton
Canada, TG6 2G1
E-mail : aweiss@math.ualberta.ca