TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 311, Number 2, February 1989

ON THE MONOID OF TAME EXTENSIONS

CORNELIUS GREITHER AND D. K. HARRISON

ABSTRACT. This paper deals with not necessarily maximal orders in abelian extensions of number fields. We restrict our attention to orders invariant under the Galois group G. Based on recent work of Childs and Hurley [CH], we introduce a notion of *tameness* for such orders (actually this is done in a slightly more general setting). The maximal order is tame in this sense if and only if the field extension is tamely ramified.

INTRODUCTION

The main idea is to define a product $*$ of two tame orders with given Galois group G and base ring R. On the isomorphism classes, this product gives the structure of a commutative monoid $\mathrm{TO}(R, G)$ with the cancellation property. $\mathrm{TO}(R, G)$ is a submonoid of a certain abelian group $\mathrm{TPO}(R, G)$, which consists of so-called preorders. For R a local number ring (i.e., R =integers in a local field) both $\mathrm{TO}(R, G)$ and $\mathrm{TPO}(R, G)$ are described in detail. $\mathrm{TPO}(R, G)$ turns out to be finitely generated.

This can be applied as follows: Let R be a local number ring, $K = \mathrm{Quot}(R)$, $L \mid K$ abelian, S the ring of integers in L. One is interested in determining all tame orders A in L which are G-invariant. (For $L = K(\sqrt{a})$, $a \in R^*$ square free, and 2 not the residual characteristic of R, it is, for example, well known that all A have the form

$$A = A_n = R \oplus \pi^n \cdot \sqrt{a} R.$$

(π is a uniformizing parameter of R, n running over all natural numbers ≥ 1.) All A occur in the form $S * A_0$ with A_0 a preorder in the trivial Galois extension $K \times \cdots \times K$ ($|G|$ factors), and the eligible A_0 can be calculated explicitly. The procedure is to assign a "string of integers" $\varphi(A)$ to each preorder (§3). Not all strings may occur, and it is not clear from the outset which strings belong to *orders*. Without going into too much detail, we can only refer to §5 and give one modest example: Suppose G is cyclic of order p and the residue characteristic of R is not p. Then there is a "visible" order $A_1 \subset R \times \cdots \times R \subset K \times \cdots \times K$, namely $A_1 = R \cdot (1, \ldots, 1) \oplus \pi \,\mathrm{Ker}(\mathrm{tr})$, where $\mathrm{tr}(r_1, \ldots, r_p) = \sum_{i=1}^{p} r_i$ is the trace. Then *all* G-invariant tame orders in L

Received by the editors November 8, 1987.
1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 12B10; Secondary 12A55.

are gotten in the form

$$A = A_n = S * A_1 * \cdots * A_1 \quad (n \text{ times}).$$

The following notation will be used throughout:

If the group G operates on the ring S, then $S^G = \{s \in S \mid \sigma(s) = s \forall \sigma \in G\}$. If R is another ring, $E_G(R)$ will denote the ring of all functions $f: G \to R$. G operates on the R-algebra $E_G(R)$ by $(\sigma f)(\tau) = f(\sigma^{-1}\tau)$.

If the finite group G acts on S, the *trace* is defined by

$$\mathrm{tr}_G(s) = \sum_{\sigma \in G} \sigma(s) \quad \text{for all } s \in S.$$

The set of all G-Galois extensions of R (up to G-isomorphism) is denoted by $\mathrm{Gal}(R, G)$.

0. Outline and results

Developing a theory of tame orders entails a certain amount of formalism (e.g., functoriality properties). The load will not become essentially lighter if we restrict to the case $R = \mathcal{O}_k$, K local field (which is the case we are ultimately interested in). Therefore we chose to give the abstract theory in general and tell the reader in this section what the underlying ideas are.

Our interest is in G-invariant R-orders $A \subset L$ ($R = \mathcal{O}_k$, K local field, L/K G-galois in the sense of [CHR]).

Noether's theorem (slightly generalized from the classical case where L, too, is a field) tells us that L/K is tame if and only if $A_0 = \mathcal{O}_L$ has a normal base. We turn this around and *define* $A \subset L$ to be *tame* if ${}_{RG}A \cong RG$. It turns out that the collection of all tame orders $A \subset L$, L/K G-galois, mod G-isomorphism, form a *monoid* $\mathrm{TO}(R, G)$. This monoid satisfies the cancellation property. To prove this (important) result we need to embed it into a *group* of so-called tame preorders $\mathrm{TPO}(R, G)$. A preorder is the same as an order, except we do not claim $1 \in A$ and $A \cdot A \subset A$. One might also say "lattice". To get a group, we must only consider tame preorders, and it is a technical problem to find the "good" definition of tameness for preorders. (The naive definition ${}_{RG}A \cong RG$ is too weak for preorders. See §1.)

§1 introduces preorders, tameness, and the monoid structure on TPO. The functoriality properties may be skipped at first reading. In §2, we come to orders and we prove they form a cancallative monoid by showing TPO is a group and $\mathrm{TO} \hookrightarrow \mathrm{TPO}$.

§§3–5 contain our results on TO and TPO for $R = \mathcal{O}_k$, K local, and arbitrary finite abelian G. In §3 we construct the map

$$\varphi: \mathrm{TPO}(R, G) \to \mathrm{Map}(\mathrm{Sim}(k, G), (1/n)\mathbf{Z})$$

where k is the residue class field of R, $\mathrm{Sim}(k, G)$ the set of simple kG-modules mod isomorphism, and $n = |G|$. Again one needs a lot of obvious but technical properties of $\varphi = \varphi_{R,G}$. The kernel of φ is canonically isomorphic

to the group of unramified G-extensions of K, hence is well known. §4 speaks about $\mathrm{Im}(\varphi)$. The most interesting question is, however, the determination of $\mathrm{Im}(\varphi \mid \mathrm{TO}) \subset \mathrm{Im}(\varphi)$. This is done in §5. One gets a description of $\mathrm{TO}(R, G)$ as an extension of the describable monoid $\mathrm{Im}(\varphi \mid \mathrm{TO})$ by the known group $\mathrm{Ker}(\varphi)$.

1. Tame preorders

Let G be a finite abelian group, R a Dedekind domain with quotient field $K = \mathrm{Quot}(R)$.

Definition 1.1. A *G-preorder* (over R) is a pair (A, L), where L is a G-Galois extension of K (not necessarily a field) and $A \subset L$ is a G-invariant lattice. (A *lattice* in L is a finitely generated R-submodule of L whose K-span is all of L.)

Example 1.2. Take R to be the ring of integers in some number field K, L a G-Galois field extension of K, and $A \subset L$ the maximal order in L.

Definition 1.3. (a) Suppose R is local with residue characteristic p. Then a G-preorder (A, L) is called *tame* if:

(i) A is an invertible RG-module with its natural structure of an RG-module,

(ii) $G = G_p \times H$, $|G_p|$ a power of p and $(p, |H|) = 1$; then $A^H = A \cap L^H$ is a separable R-algebra and $A^H \cdot A \subset A$.

Remark. (i) is of a technical nature and will disappear as soon as we consider orders, not preorders.

(b) If R is local with residue characteristic 0, *all* preorders are called tame. (We will not see this case in §§3–5.)

Definition 1.4. A G-preorder (A, L) over R is tame if (A_m, L) is tame over R_m for all maximal ideals $m \subset R$.

Example 1.5. If R is a ring of integers, $L \mid K$ unramified, A the maximal order in L, then $A \mid R$ is G-Galois, and this is known to imply 1.3(i) and (ii). (Normal bases exist locally in Galois extensions.)

Now we define a *product* $*$ of G-preorders.

Definition 1.6. Let (A, L) and (B, M) be G-preorders over R. Define $A * B$ to be the R-module

$$A * B = \left\{ \sum a_i \otimes b_i \in A \otimes_R B \mid \forall \sigma \in G \sum \sigma a_i \otimes \sigma^{-1} b_i = \sum a_i \otimes b_i \right\}$$
$$= (A \otimes_R B)\Delta \quad \text{with } \Delta = \{(\sigma, \sigma^{-1}) \mid \sigma \in G\} \subset G \times G.$$

Define $L * M \subset L \otimes M$ analogously. Let $\sigma(\sum a_i \otimes b_i) = \sum \sigma a_i \otimes b_i$ $(= \sum a_i \otimes \sigma b_i)$ for all $\sum a_i \otimes b_i \in A * B$, $\sigma \in G$.

Proposition 1.7. (a) $(A * B, L * M)$ *is a* G*-preorder.* (b) $*$ *is commutative and associative up to isomorphism, and* $(E_G(R), E_G(K))$ *is neutral under* $*$. (c) *The set of isomorphism classes of* G*-preorders over* R *is a commutative monoid, which we call* $\mathrm{PO}(R, G)$. (d) *The tame* G*-preorders form a submonoid* $\mathrm{TPO}(R, G)$ *of* $\mathrm{PO}(R, G)$.

Proof. (a) Since R is Dedekind, ${}_RA$ and ${}_RB$ are flat, so

$$A * B \subset A \otimes_R B \subset L \otimes_k M.$$

One easily sees $K \cdot (A * B) = L * M$, and $A * B$ is R-finitely generated (since $A \otimes B$ is) and G-invariant. It is well known that $L * M$ is again a G-Galois extension (see [H]; $*$ is actually the product in $\mathrm{Gal}(K, G)$).

(b) Easy verification.

(c) Follows from (b).

(d) Suppose (A, L) and (B, M) are p-tame; we want to show that $(A*B, L * M)$ is p-tame. Let us verify conditions (i) and (ii) in 1.3.

(i) We may suppose R local. Then invertible RG-modules and free cyclic RG-modules are the same, hence

$$A * B = (A \otimes_R B)^{\Delta} \cong {}_{RG}(RG \otimes_R RG)^{\Delta},$$

and it is easily checked that the latter expression is RG-isomorphic to RG.

(ii) Again suppose R local, of residue characteristic $p > 0$, $G = G_p \times H$ as above. We have $(A * B)^H = ((A \otimes B)^{\Delta})^H = ((A \otimes B)^{H \times H})^{\Delta}$. Now since A and B are R-flat, $(A \otimes B)^{H \times H} = A^H \otimes B^H$. Thus $(A * B)^H = A^H * B^H$, $*$ formed with the Galois group G/H. But $*_{G/H}$ is the product in the abelian group $\mathrm{Gal}(R, G/H)$ of G/H-Galois extensions of R. A^H and B^H are in $\mathrm{Gal}(R, G/H)$ because they are R-separable orders in the G/H-extensions L^H and M^H of K, by hypothesis. Thus $C = A^H * B^H = (A * B)^H$ is a separable algebra. The property $C \cdot (A*B) \subset A*B$ follows from $A^H \cdot A \subset A$, $B^H \cdot B \subset B$.

Before studying the monoids (groups, as we shall prove) $\mathrm{TPO}(-, -)$ more closely, we examine their functorial behavior in both arguments. (We already used localizing of the first argument.)

Definition 1.8. Let $f\colon R \to S$ be an injective ring homomorphism of Dedekind rings. Note S is R-flat. Define

$$\mathrm{PO}(f, G)\colon \mathrm{PO}(R, G) \to \mathrm{PO}(S, G)$$

by

$$(A, L) \mapsto (S \otimes_R A, \mathrm{Quot}(S) \otimes_k L).$$

Proposition 1.9. (a) $\mathrm{PO}(-, G)$ *is a functor to the category of monoids.* (b) $\mathrm{PO}(f, G)$ *maps* $\mathrm{TPO}(R, G)$ *into* $\mathrm{TPO}(S, G)$.

Proof. (a) It is easy to check that PO is a functor to sets. We want it to preserve the $*$-product. One may verify this using the flatness of S over R. $S \otimes_R$- preserves kernels, and therefore it commutes with $(-)^{\Delta}$. It is also easy to see that $\mathrm{PO}(f, G)(E_G(R)) \cong E_G(S)$.

(b) Suppose (A, L) tame and R local; we want $(S \otimes_R A, \mathrm{Quot}(S) \otimes_K L)$ to be tame. First consider condition (i). We have

$$S[G](S \otimes_R A) \cong S[G] \otimes_{R[G]} A \cong S[G] \otimes_{R[G]} R[G] \cong S[G].$$

For (ii) note that $(S \otimes A)^H = S \otimes_R A^H$. From this everything follows.

Definition 1.10. Now let $\varphi: G \to \tilde{G}$ be a homomorphism of finite abelian groups. Define

$$\mathrm{PO}(R, \varphi): \mathrm{PO}(R, G) \to \mathrm{PO}(R, \tilde{G})$$

by

$$(A, L) \mapsto ((A \otimes_R E_{\tilde{G}}(R))^{\Delta(\varphi)}, (L \otimes_K E_{\tilde{G}}(K))^{\Delta(\varphi)})$$

where $\Delta(\varphi) = \{(\sigma^{-1}, \varphi(\sigma) \mid \sigma \in G\} \subset G \times \tilde{G}$.

Proposition 1.11. (a) $\mathrm{PO}(R, -)$ *is a functor from finite abelian groups to commutative monoids.*

(b) $\mathrm{PO}(R, \varphi)$ *maps* $\mathrm{TPO}(R, G)$ *into* $\mathrm{TPO}(R, \tilde{G})$.

Proof. (a) From Galois theory of rings, as used in [H], one has that $(L \otimes_K E_G(K))^{\Delta(\varphi)}$ is a G-Galois extension of K (it is $T(R, \varphi)(L)$ in the notation of [H]). The property $\mathrm{PO}(R, \varphi) \circ \mathrm{PO}(R, \psi) = \mathrm{PO}(R, \varphi\psi)$ is a rather long but straightforward calculation. Another long calculation yields that $\mathrm{PO}(R, \varphi)$ is indeed a monoid homomorphism.

(b) Suppose (A, L) tame, and let $(B, M) = \mathrm{PO}(R, \varphi)(A, L)$. Suppose R local and let us verify 1.3(i), that is, B is free cyclic over $R\tilde{G}$:

$$\begin{aligned} B &\cong_{R\tilde{G}} (A \otimes_R E_G(R))^{\Delta(\varphi)} \cong (RG \otimes_R E_{\tilde{G}}(R))^{\Delta(\varphi)} \quad \text{(hypothesis)} \\ &\cong (E_G(R) \otimes_R E_{\tilde{G}}(R))^{\Delta(\varphi)} (E_G(R) \cong_{RG} RG) \\ &\cong E_{\tilde{G}}(R) \quad \text{(direct calculation)}. \end{aligned}$$

Let us also check condition (ii). Let $\tilde{G} = \tilde{G}_p \times \tilde{H}$, $|\tilde{G}_p|$ a power of p, $p \nmid |\tilde{H}|$. Then $\varphi(H) \subset \tilde{H}$. Let $C = B^{\tilde{H}}$, $\Delta = \Delta(\varphi)$. Then

$$\begin{aligned} C &= (A \otimes E_{\tilde{G}}(R))^{\Delta(e \times \tilde{H})} \\ &= (A \otimes E_{\tilde{G}}(R))^{(H \times e) \cdot \Delta \cdot (e \times \tilde{H})} \quad (\text{since } H \times e \subset \Delta \cdot (e \times \tilde{H})) \\ &= (A^H \otimes E_{\tilde{G}}(R))^{\Delta(e \times \tilde{H})} \quad (E_{\tilde{G}}(R) \ R\text{-flat}). \end{aligned}$$

$A^H \otimes E_{\tilde{G}}(R)$ is a separable R-algebra with Galois group $G/H \times \tilde{G}$ over R. By Galois theory of rings, $C = (A^H \otimes E_{\tilde{G}}(R))^{\Delta(e \times \tilde{H})}$ is also a separable algebra. The property $C \cdot B \subset B$ is verified easily.

The next two objectives are:

(1) Introducing a submonoid $\mathrm{TO} \subset \mathrm{TPO}$ which consists of the so-called orders. These orders are the object of main interest.

(2) Proving TPO is a group. This gives cancellation for the monoid TO, which itself is practically never a group.

2. Tame orders and the group TPO

Let G and R be as in the last section.

Definition 2.1. If (A, L) is a G-preorder over R, we say that (A, L) is an *order* if A is closed under multiplication and contains 1, that is, A is an R-algebra. The set of isomorphism classes of tame G-orders over R is called $\mathrm{TO}(R, G)$.

Remark 2.2. $\mathrm{TO}(-,-)$ is a subbifunctor of $\mathrm{TPO}(-,-)$.

Proof. The $*$-product of two algebras is again an algebra.

Our orders are just the G-invariant orders ("order" understood in the number-theoretical sense), if R is a number ring.

Theorem 2.3. *Let (A, L) be an order and $\mathrm{char}(R) = 0$. Then (A, L) is tame if and only if condition* (i) *in* 1.3 *is satisfied. (This means that condition* (ii) *is automatic here.)*

Proof. We introduce an auxiliary notion: Call (A, L) *semitrivial* if $L \cong E_G(K)$, the trivial element of the group $\mathrm{Gal}(K, G)$. First we prove the theorem for semitrivial (A, L). We may suppose R local, since tameness is defined via the local case. We have to deduce (ii) from (i). By [CH, Theorem 4.1], A is a "tame RG-object," and this encompasses by definition [CH] that the trace map $\mathrm{tr}_G: A \to R$ is onto. We have to prove that $B = A^H$ is a separable algebra (trivially $BA \subset A$,—because A is an algebra). A^H is a finite algebra contained in $L^H \cong E_{G_p}(K)$ (see §1 for $G = G_p \times H$). Thus $A^H \subset E_{G_p}(R)$ since $E_{G_p}(R)$ is integrally closed and A^H/R is finite. We factor tr_G in the form

$$\mathrm{tr}_G: A \xrightarrow[\mathrm{tr}_H]{} A^H \xrightarrow[\mathrm{tr}_{G_p}]{} R.$$

Since tr_G is onto, also $\mathrm{tr}_{G_p}: A^H \to R$ is onto. Therefore by Lemma 2.4 $A^H = E_{G_p}(R)$; hence A^H is R-separable.

Lemma 2.4. *Let R be local with residue characteristic p, G_p a finite abelian p-group, and $C \subset E_{G_p}(R)$ a G_p-invariant R-order. Then*

$$\mathrm{tr}_{G_p}: C \to R \text{ is onto } \Leftrightarrow C = E_{G_p}(R).$$

Proof. $\Leftarrow$ holds trivially. For the reverse, let $\overline{R} = R/Ra(R)$, $\pi: E_{G_p}(R) \to E_{G_p}(\overline{R})$ the canonical projection. By Nakayama's Lemma, it suffices to show that $\pi(C) = E_{G_p}(\overline{R})$. Now $\pi(C)$ is an $\overline{R}G_p$-submodule of $E_{G_p}(\overline{R})$, and $E_{G_p}(\overline{R}) \cong \overline{R}G_p$ canonically as $\overline{R}G_p$-modules. Since $\overline{p} = 0$, $\overline{R}G_p$ has exactly one maximal ideal. It coincides with the nil radical and has the form

$$I = \left\{ \sum_{G_p} \overline{r}_\sigma \cdot \sigma \mid \sum \overline{r}_\sigma = 0, \overline{r}_\sigma \in \overline{R} \right\}.$$

One sees that under the canonical isomorphism $E_{G_P}(\overline{R}) \cong \overline{R}G_p$, I corresponds with $\ker(\mathrm{tr}_{G_P})$. Therefore $\pi(C) = E_{G_P}(\overline{R}) \Leftrightarrow \pi(C)$ is not contained in $\ker(\mathrm{tr}_{G_p})$, $\Leftrightarrow$ tr is not zero on $\pi(C)$, $\Leftrightarrow C$ contains an element of trace 1.

Now we still must prove the theorem in the general case. Let S be any faithfully flat R-algebra which is Dedekind, $j: R \subset S$. It is fairly easy to see that (A, L) is tame if and only if $\mathrm{PO}(j, G)(A, L)$ is tame. (The if part is Proposition 1.9(b), and the only if part is done similarly, using descent.) Therefore by the above it is enough to see that there exists $S \mid R$ faithfully flat Dedekind, such that $\mathrm{PO}(j, G)(A, L)$ is semitrivial. Here one can take $S =$ maximal R-order in E, where E is any separable finite field extension of K which splits L. Q.E.D.

The next objective is to prove that $\mathrm{TPO}(R, G)$ is a (commutative) group. For technical reasons, we again restrict ourselves to the case $\mathrm{char}(R) = 0$. Let $|G| = n$. From now on, we suppress L in the notation for (A, L).

For A a tame preorder, we define

$$A^{\perp} = \{x \in L \mid \mathrm{tr}_G(x \cdot A) \subset R\}.$$

$A^{\perp}$ is G-invariant. Since $\mathrm{tr}(xy)$ is a nondegenerate bilinear form, $A^{\perp}$ is an R-lattice in L. Therefore $A^{\perp}$ is again a preorder. We can define a map

$$j: A \otimes_R A^{\perp} \to E_G(K)$$

by

$$j(a \otimes b) = (\sigma \mapsto (1/n)\,\mathrm{tr}(\sigma^{-1}a \cdot b)).$$

$A^{\perp}$ is not quite the $*$-inverse of A, but "almost." Let $A^{-\perp}$ ("A to the minus perp") be $A^{\perp}$ as an R-module, with G operating via the inverse map $G \to G$.

Theorem 2.5. *If* $\mathrm{char}(R) = 0$, $\mathrm{TPO}(R, G)$ *is an abelian group. The inverse of* A *is* $A^{-\perp}$, *and*

$$j: A * A^{-\perp} \to E_G(K)$$

induces a G*-isomorphism* $A * A^{-\perp} \xrightarrow{\cong} E_G(R)$. (N.B. *for* A *not tame,* $A^{-\perp}$ *is defined all the same, but we do not know whether it is inverse to* A.)

Proof. First we assume that A is semitrivial (i.e., $A \subset L = E_G(K)$) and that R contains a primitive nth root ζ of unity. We claim j is an isomorphism onto $E_G(R)$. For this, it is necessary and sufficient that

$$j_m: A_m * (A^{-\perp})_m \to E_G(K) \quad \text{is an isomorphism onto } E_G(R_m) \quad \forall m.$$

Now $A_m = \mathrm{PO}(R \hookrightarrow R_m, G)(A)$, and $(\ )^{\perp}$ commutes with localization. Therefore it is enough to establish our claim for local R.

Let us identify $E_G(K)$ with $E_{G_P}(E_H(K))$. (Recall $p = \mathrm{char}(R/Ra(R))$, $G = G_p \times H$, $|G_p|$ a power of p, $|H|$ not divisible by p.)

Lemma 2.6. *There exists an H-preorder $A_0 \subset E_H(K)$ such that $A = E_{G_p}(A_0)$.*

Proof. For any ring T, $E_{G_p}(T) = \bigoplus_{\sigma \in G_p} Te_\sigma$, where e_σ is defined by $e_\sigma(\tau) = \delta_{\sigma\tau}$. The e_σ are idempotent. Now $A^H = A \cap L^H = A \cap (E_{G_p}(E_H(K)))^H = A \cap E_{G_p}(K)$ (where we identify K with the diagonal in $E_H(K)$). Since A is tame, A^H is a separable R-algebra. Because R is integrally closed and A^H is integral over R, A^H is contained in $E_{G_p}(G)$. A^H is a G_p-Galois extension of R, since it is a separable G-invariant order in $E_{G_p}(K)$. Therefore the inclusion $A^H \subset E_{G_p}(R)$ is a morphism of G_p-Galois extensions and hence an isomorphism, that is, $A^H = E_{G_p}(R) = \bigoplus_{\sigma \in G_p} Re_\sigma$. Hence $A = A^H \cdot A = \bigoplus_{\sigma \in G_p} A \cdot e_\sigma$, and $A \cdot e_\sigma$ is up to canonical isomorphism a subalgebra of $E_H(K)$. Since A is Gp-invariant, all algebras $A \cdot e_\sigma$ must be equal to one subalgebra $A_0 \subset E_H(K)$, and we get $A = E_{G_p}(A_0)$.

Lemma 2.7. *$E_{G_p}(A_0)^{-\perp} \cong E_{G_p}(A_0^{-\perp})$ canonically, where in forming $A_0^{-\perp}$ one naturally uses tr_H in the place of tr_G, and $E_{\overline{G_p}}(-)$ is $E_{G_p}(-)$ with G_p operating through the inverse.*

Proof. Easy to check.

In the next diagram, we provide subscripts G and H for the symbols j and $*$ for clarity:

$$\begin{array}{ccc} A *_G A^{-\perp} & \xrightarrow{j_G} & E_G(K) \\ \| & & \| \\ E_{G_p}(A_0) *_G E_{\overline{G_p}}(A_0^{-\perp}) & \xrightarrow{j_G} & E_{G_p}(E_H(K)) \\ \cong \uparrow \alpha & & \| \\ E_{G_p}(A_0 *_H A_0^{-\perp}) & \xrightarrow{E_{G_p}(j_H)} & E_{G_p}(E_H(K)). \end{array}$$

The isomorphism α is the composite

$$E_{G_p}(A_0 *_H A_0^{-\perp}) \overset{\alpha_0}{\underset{\cong}{\rightarrow}} (E_{G_p}(R) *_{G_p} E_{\overline{G_p}}(R)) \otimes (A_0 *_H A_0^{-\perp}) \downarrow \text{canonical isom.} \; E_{G_p}(A_0) *_G E_{\overline{G_p}}(A_0^{-\perp}),$$

where

$$\alpha_0(e_\sigma) = \sum_{\substack{\tau, \rho \in G_p \\ \tau\rho = \sigma}} e_\tau \otimes e_{\rho^{-1}} \quad \text{for all } \sigma \in G.$$

Lemma 2.8. *The above diagram consists of G-maps and commutes.*

Proof. The G-equivariance is easy to check. We check the commutativity of the lower rectangle. Let us begin with an element

$$x = e_\sigma \cdot \sum_i b_i \otimes c_i, \quad \sigma \in G_p, \; b_i \in A_0, \; c_i \in A_0^{-\perp}, \quad \sum_i b_i \otimes c_i \in A_0 *_H A_0^{-1}.$$

Then $\alpha(x) = \sum_{\tau\rho=\sigma} \sum_i (e_\tau b_i) \otimes (e_{\rho^{-1}} c_i)$. Recall the definition of j_G: $j_G(u \otimes v) = (1/|G|) \sum_{g \in G} \mathrm{tr}_G(g^{-1}u \cdot v) \cdot e_g$. Thus we get

$$
\begin{aligned}
j_G(\alpha(x)) &= \frac{1}{|G|} \sum_{\substack{\tau\rho=\sigma \\ \tau,\rho \in Gp}} \sum_i \sum_{\gamma \in G_\rho} \sum_{h \in H} [\mathrm{tr}_G((\gamma h)^{-1}(e_\tau b_i) \cdot e_{\rho^{-1}} c_i) e_h e_\gamma] \\
&= \frac{1}{|G|} \sum_{\tau\rho=\sigma} \sum_i \sum_\gamma \sum_h [\mathrm{tr}_G(e_{\tau\gamma^{-1}} e_{\rho^{-1}} h^{-1}(b_i) c_i) \cdot e_h \cdot e_\gamma] \\
&= \frac{1}{|G|} \sum_\rho \sum_i \sum_h [\mathrm{tr}_G(e_{\rho^{-1}} \cdot h^{-1}(b_i) c_i)] e_h e_\sigma \qquad (t = \rho^{-1}\sigma, \gamma = \sigma) \\
&= \frac{1}{|G|} \sum_\rho \sum_i \sum_h [\mathrm{tr}_H(h^{-1}(b_i) c_i)] e_h e_\sigma \qquad (\mathrm{tr}_{G_\rho}(e_{\rho^{-1}}) = 1) \\
&= \frac{1}{H} \left(\sum_i \sum_h \mathrm{tr}_H(h^{-1}(b_i) \cdot c_i) \cdot e_h \right) e_\sigma \\
&= E_{G_\rho}(j_H) \left(e_\sigma \cdot \sum_i b_j \otimes c_i \right). \quad \text{Q.E.D.}
\end{aligned}
$$

Remember we assumed A semitrivial, and ζ, a primitive nth root of unity, is in R. R is a local Dedekind ring with maximal ideal generated by π, say. By Lemma 2.8 we may, in proving j_G an isomorphism, replace G by H; that is, we may assume $G = H$. Then $n = |G|$ is a unit in R, and the elements $v_\chi = (1/n)(x(g))_{g \in G}$ are a set of minimal orthogonal idempotents in RG (χ running over all characters $G \to R^*$). Therefore every RG-submodule $I \subset RG$ has the form $I = \bigoplus_\chi \pi^{f}(x) \cdot R v_\chi$ with $f(\chi) \in \mathbf{N} \cup \{\infty\}$ and π^∞ is defined to be zero. Similarly, every RG-submodule J of $E_G(R)$ has the form

$$
J = \bigoplus_\chi \pi^{f(x)} R\omega_\chi, \omega_\chi = \frac{1}{n} \sum \chi(g) e_g, \qquad f(\chi) \in \mathbf{N} \cup \{\infty\}.
$$

From this, and since A is a preorder in $E_G(K)$, we get

$$
A = \bigoplus_\chi \pi^{f(x)} R\omega_\chi \quad \text{with } f(\chi) \in \mathbf{Z}.
$$

Lemma 2.9. $A^\perp = \bigoplus_\chi \pi^{-f(x)} R\omega_\chi$.

Proof. This is a straightforward calculation, using $n \in R^*$ and $\mathrm{tr}_G(W_\chi \cdot W_\theta) = n$ for $\chi \cdot \theta = 1$ and 0 otherwise.

We define a map

$$
\lambda: E_G(R) \to A \otimes A^{-\perp},
$$

$$
\omega_x \mapsto \pi^{f(x)} \omega_x - 1 \oplus \pi^{-f(x)} \omega_x.
$$

Obviously λ is injective. Using the formula $\sigma(\omega_\chi) = \omega(\sigma) \cdot \omega_\chi$ for $\sigma \in G$, one checks that

$$
\mathrm{Im}(\lambda) = A *_G A^{-\perp}.
$$

Thus the theorem (in case A is subtrivial, $\zeta \in R$) will follow if we can show $j\lambda = \mathrm{id}$ on $E_G(R)$.

Take $\omega_x \in E_G(R)$. We calculate $j\lambda(\omega_x) = j(\pi^{f(x)}\omega_x - 1 \otimes \pi^{-f(x)}\omega_x)$:

$$\begin{aligned} j\lambda(\omega_x) &= \frac{1}{|G|}\sum_\sigma \mathrm{tr}_G(\sigma^{-1}(\pi^{f(x)}\omega_x^{-1}) \cdot \pi^{-f(x)}\omega_x) \cdot e_\sigma \\ &= \frac{1}{|G|}\sum_\sigma \mathrm{tr}_G(\sigma^{-1}(\omega_x - 1) \cdot \omega_x) e_\sigma \\ &= \frac{1}{|G|}\sum_\sigma \mathrm{tr}_G(x^{-1}(\sigma^{-1})) e_\sigma \\ &= \frac{1}{|G|}\sum_\sigma |G| \cdot x(\sigma) e_\sigma = \sum_\sigma x(\sigma) e_\sigma = \omega_x . \end{aligned}$$

This proves Theorem 2.5 in case A is subtrivial and $\zeta_n \in R$. The general case is deduced as follows: Let incl: $R \subset S$ be an inclusion of Dedekind rings such that $S \otimes_R A$ $(= \mathrm{PO}(\mathrm{incl}, G)(A))$ is semitrivial and S contains a primitive nth root of unity ζ. (Take for S the maximal R-order in $M(\zeta_n)$, where $M \mid K$ is a finite separable field extension splitting L.) Then one verifies that $S \otimes j_R$ is just j_S. Thus, the statement "j_S injective and $\mathrm{Im}(j_S) = E_G(S)$" implies "$j_R$ injective and $\mathrm{Im}(j_R) = E_G(R)$" by faithfully flat descent.

Corollary 2.10. *The monoid* $\mathrm{TO}(R, G)$ *has the cancellation property (for all finite abelian groups* G *and all Dedekind rings* R *of characteristic zero).*

3. The map φ and its kernel

In this section, R is assumed to be a "complete number ring," i.e., the ring of integers in a local number field ($\mathbf{R}$ and $\mathbf{C}$ excluded, of course).

Notation 3.0. Let $Ra(R) = \pi \cdot R$ and $k = R/\pi R$, $p = \mathrm{char}(k)$, $G = G_p \times H$ as usual (G_p a p-group, $p \nmid |H|$).

We want to define a group homomorphism $\varphi = \varphi_{R,G}$ from $\mathrm{TPO}(R, G)$ into an explicitly given group and study its kernel. In later sections, we shall examine the image of φ and $\varphi(\mathrm{TO}(R, G))$ (recall $\mathrm{TO} \subset \mathrm{TPO}$). Since RH is π-adically complete, the canonical map

$$\{e \in RH \mid e \text{ idempotent}\} \to \{e \in kH \mid e \text{ idempotent}\}$$

is bijective. Write

$$RH = \bigoplus_{i=1}^{m} e_i RH, \quad \{e_1, \ldots, e_m\} \text{ a complete orthogonal set of minimal idempotents.}$$

Then the e_i are also a complete set of minimal idempotents. Since kH is semisimple, this means that $e_i KH = (e_i RH)/(\pi e_i RH)$ is a field. Hence $e_i RH$ is a local ring with π as a parameter; call this local ring R_i. As is well known,

all nonzero ideals of $e_i RH$ are generated by a power of π. Thus, every ideal $I \subset RH$ with $KI = KH$ has the form

$$I = \bigoplus_{i=1}^{m} \pi^{f_i} R_i, \qquad f_i \in \mathbf{N}.$$

Via the canonical RH-isomorphism $\eta: RH \to E_H(R)$ with $\eta(\sigma) = e_\sigma$, we also get an RH-decomposition $E_H(R) = \bigoplus S_i$, $S_i = \eta(R_i)$. Every preorder $A \subset E_H(K)$ has the form

$$A = \bigoplus_{i=1}^{m} \pi^{f_i} S_i, \qquad f_i \in \mathbf{Z},$$

and all such A are preorders. So we have achieved a *description of all semitrivial H-preorders by a finite sequence of integers.* The map φ is just a generalization of this idea.

First, the index set $\{1, \ldots, m\}$ is in bijective correspondence with the set of (isomorphism classes of), simple kH-modules.

Definition 3.1. The set of simple kH-modules is called $\mathrm{Sim}(k, H)$. (Note here "simple"="irreducible," since kH is semisimple.)

Thus, we defined an "invariant map"

$$\varphi_0(R, H): \mathrm{TPO}_0(R, H) = \{A \in \mathrm{TPO}(R, H) \mid A \text{ semitrivial}\} \to \mathrm{Map}(\mathrm{Sim}(k, H), \mathbf{Z}).$$

Second, we showed before (2.6) that every tame G-preorder A is of the form

$$A = E_{G_P}(A_0)$$

with A_0 an H-preorder in $E_H(K)$. A_0 is obviously unique, and the canonical map $\mathrm{TPO}_0(R, H) \ni A_0 \mapsto E_{G_P}(A_0) \in \mathrm{TPO}_0(R, G)$ is an isomorphism of groups. From representation theory, it is known that $\mathrm{Sim}(k, H) \xrightarrow{\cong} \mathrm{Sim}(k, G)$ canonically (as sets). Therefore the above invariant map $\varphi_0(R, H)$ is defined for G in the place of H also.

Now we define the map $\varphi(R, G): \mathrm{TPO}(R, G) \to \mathrm{Map}(\mathrm{Sim}(k, G), (1/n)\mathbf{Z})$ $(n = |G|)$ in the following way: given $(A, L) \in \mathrm{TPO}(R, G)$, consider $(B, M) =$ n-fold $*$-product of (A, L) with itself. Define (note B is semitrivial since $\mathrm{Gal}(K, G)$ is n-torsion!)

$$\varphi(R, G)(A, L) = (1/n)\varphi_0(B, M).$$

Note first that φ is independent of the choice of the parameter π. We intend to show (Theorem 3.3) that φ is a group homomorphism (the group structure on $\mathrm{Map}(\mathrm{Sim}(K, G), \mathbf{Z})$ coming from addition in $\mathbf{Z}$). But before this, we need functoriality of φ.

Let $t: R \to T$ be an injective ring homomorphism of complete number rings. Then t yields an inclusion of the residue class fields $k \subset \tilde{k} = T/Ra(T)$. We

have that π is associated to ψ^e, where $e \in \mathbf{N}$ and ψ is a parameter of T. There is a canonical map

$$t^{\#}\colon \operatorname{Sim}(\tilde{k}, G) \to \operatorname{Sim}(k, G)$$

defined as follows: $t^{\#}(N)$ is the simple kG-module M such that N is a composition factor of $\tilde{k} \otimes_k M$.

Theorem 3.2. *The following diagram commutes*:

$$\begin{array}{ccc} \operatorname{TPO}(R, G) & \overset{\varphi(R,G)}{\to} & \operatorname{Map}\left(\operatorname{Sim}(k, G), \tfrac{1}{n}\mathbf{Z}\right) \\ {\scriptstyle T\otimes_s -}\downarrow & & \downarrow{\scriptstyle e\cdot \operatorname{Map}(t^{\#}, \frac{1}{n}\mathbf{Z})} \\ \operatorname{TPO}(T, G) & \overset{\varphi(T,G)}{\to} & \operatorname{Map}\left(\operatorname{Sim}(\tilde{k}, G), \tfrac{1}{n}\mathbf{Z}\right) \end{array}$$

Proof. As in the proof of Theorem 2.5, one may assume $|G|$ prime to p, that is, $G = H$. (See Lemma 2.6.) The range of $\varphi(T, G)$ is torsion-free, and the $|G|$ th power of each element in $\operatorname{TPO}(R, G)$ is semitrivial. Therefore it is enough to take $(A, L) \in \operatorname{TPO}(R, G)$ semitrivial and show it maps to the same element both ways. Write

$$A = \bigoplus_{M \in \operatorname{Sim}(k, G)} \pi^{f(M)} \cdot S_M,$$

where $S_M = \eta(R_M)$, $R_M = e_M RG$, and $\bar{e}_M kG = M$. (In other words, R_M is the lifting of M to a projective RG-module.) Then

$$T \otimes_R A = \bigoplus_M \pi^{f(M)}(T \otimes S_M),$$

and $T \otimes S_M = \eta(T \otimes R_M)$, $T \otimes R_M = e_M \cdot TG$. Now

$$e_M \tilde{k}G = \bigoplus_{N \in \mathfrak{A}} e_N \tilde{k}G,$$

where the e_N run over the minimal idempotents in $\tilde{k}G$ which are a multiple of e_M. One checks that $\mathfrak{A}$ consists of precisely those simple $\tilde{k}G$-modules which are a direct summand of $e_M \tilde{k}G$, i.e.,

$$\mathfrak{A} = (t^{\#})^{-1}(M).$$

Therefore

$$T \otimes A = \bigoplus_{N \in \operatorname{Sim}(\tilde{k}, G)} \pi^{f(t(N))} S_N = \bigoplus \psi^e \cdot f(t^{\#}(N)) \cdot S_N,$$

that is, $\varphi(T, G)(T \otimes A) = (N \mapsto e \cdot f(t^{\#}N))$.

Chasing the diagram the other way gives the same result.

Theorem 3.3. *$\varphi(R, G)$ is a group homomorphism.*

Proof. As in the last proof, one may suppose $|G|$ prime to $p = \operatorname{char}(k)$; that is, $n = |G|$ is invertible in R.

Let $T \supset R$ be a complete number ring containing an n th root ζ of unity, let $t\colon R \subset T$ be the inclusion, $\tilde{k} = T/Ra(T)$. Then $t^{\#}\colon \mathrm{Sim}(\tilde{k}, G) \to \mathrm{Sim}(k, G)$ is surjective (by construction of $t^{\#}$). Thus $\mathrm{Map}(t^{\#}, (1/n)\mathbf{Z})$ is an injective group homomorphism, and by Theorem 3.2 it is enough to show that $\varphi(T, G)$ is a group homomorphism. Let $\tilde{K} = \mathrm{Quot}(T)$.

As in the proof of 2.8, we write $E_G(T) = \bigoplus_\chi T \cdot \omega_\chi$, χ running over all characters from G to $\langle\zeta\rangle$,

$$\omega_\chi = (1/n)(\chi(g)), \qquad g \in G.$$

Let A and B be G-preorders over T; we have to show that $\varphi(T, G)(A * B) = \varphi(T, G)(A) + \varphi(T, G)(B)$. The semitrivial orders A^{*n} and B^{*n} can be written

$$A^{*n} = \bigoplus_\chi \pi^{f(\chi)} \cdot T \cdot \omega_\chi,$$

$$B^{*n} = \bigoplus_\chi \pi^{g(\chi)} \cdot T \cdot \omega_\chi, \quad \text{respectively.}$$

As before, we identify $\mathrm{Sim}(\tilde{k}, G)$ with the set $\{\chi\}$ of characters from G to $\{\zeta\}$. If this is done, we have

$$\varphi(T, G)(A) = (1/n)f \in \mathrm{Map}(\mathrm{Sim}(k, G), (1/n)\mathbf{Z}),$$
$$\varphi(T, G)(B) = (1/n)g.$$

Claim. $(\bigoplus_x \pi^{f(x)} \cdot T\omega_x) * (\bigoplus_x \pi^{g(x)} \cdot T \cdot \omega_x) = \bigoplus \pi^{f(x)+g(x)} \cdot T \cdot \omega_x$, where $E_G(\tilde{K}) * E_G(\tilde{K})$ is identified with $E_G(\tilde{K})$ via $\omega_x \otimes \omega_x \to \omega_x$.

Proof. This is a straightforward computation, using the rule $\sigma(\omega_x) = \omega(\sigma)\cdot\omega_x$. From the claim it follows that

$$(A * B)^{*n} = A^{*n} * B^{*n} = \bigotimes_x \pi^{f(x)+g(x)} \cdot T \cdot \omega_x,$$

that is, $\varphi(T, G)(A * B) = (1/n)(f + g)$. Q.E.D.

Corollary 3.4. *If $A \in \mathrm{TPO}(R, G)$ and m is any natural number such that A^{*m} is semitrivial, then $\varphi(R, G)(A) = (1/m)\varphi_0(A^{*m})$.*

Proof. The same argument as for φ yields that φ_0 (see above) is also a group homomorphism. Since the range of φ and φ_0 are torsion-free, it is enough to check

$$n \cdot \varphi(R, G)(A) = (n/m)\varphi_0(A^* m).$$

But $n\varphi(R, G)(A) = n\cdot(1/n)\cdot\varphi_0(A^{*n}) = (1/m)\cdot m\cdot\varphi_0(A^{*n}) = (1/m)\cdot\varphi_0(A^{*n\cdot m}) = (1/m)\cdot n\cdot\varphi_0(A^{*m})$. Now let $\psi\colon G \to G$ be a homomorphism of finite abelian groups, $n = |G|$. Then there is a natural map $\psi^{\#}\colon \mathrm{Sim}(k, G) \to \mathrm{Sim}(k, G)$ defined by $\psi^{\#}(N) =$ the (!) simple kG-module M such that M is a composition factor of $N = KG \otimes_{kG} N$. (One checks that $\psi^{\#}$ is a well-defined map.)

Theorem 3.5. *The following diagram commutes*:

$$\begin{array}{ccc} \mathrm{TPO}(R,G) & \xrightarrow{\varphi(R,G)} & \mathrm{Map}\left(\mathrm{Sim}(k,G),\tfrac{1}{n}\mathbf{Z}\right) \\ & & \downarrow \mathrm{Map}(\psi^{\#},\frac{1}{n}\mathbf{Z}) \\ \mathrm{PO}(R,\psi)\downarrow & & \mathrm{Map}\left(\mathrm{Sim}(k,\tilde{G}),\tfrac{1}{\mathrm{lcm}(n,n)}\mathbf{Z}\right) \\ & & \cup \\ & \mathrm{TPO}(R,G)\overset{\varphi(R,\tilde{G})}{\to} & \mathrm{Map}\left(\mathrm{Sim}(k,\tilde{G}),\tfrac{1}{n}\mathbf{Z}\right) \end{array}$$

Proof. As in 3.3, we assume n prime to $\mathrm{char}(k)$. Moreover we assume for simplicity that also n is prime to $\mathrm{char}(k)$. The general case is not much harder since $\mathrm{Im}(\psi)$ is automatically a subgroup of the non-p-part of G, but is more technical (invocation of Lemma 2.6). Since the abelian groups on the right-hand side are torsion-free, it is enough to consider a semitrivial $A \in \mathrm{TPO}(R,G)$ and show it maps to the same thing both ways. Write

$$A = \bigoplus_M \pi^{f(M)} \cdot S_M, \qquad M \in \mathrm{Sim}(k,G) \quad \text{(see beginning of this section)}.$$

Then

$$\begin{aligned} \mathrm{PO}(R,\psi)(A) &= A * E_{\tilde{G}}(R) \\ &= \left(A \otimes_R, E_{\tilde{G}}(R)\right)^{\Delta(\psi)}, \qquad \Delta(\psi) = \{(\sigma^{-1}, \psi(\sigma)), \sigma \in G\}, \\ &= \left(\bigoplus_M (\pi f^{(M)} S_M \otimes_R E_{\tilde{G}}(R))\right)^{\Delta(\psi)} \\ &= \bigoplus_M \pi^{f(M)} \cdot (S_M \otimes_R E_{\tilde{G}}(R))^{\Delta(\psi)}. \end{aligned}$$

Denote $(S_M \otimes_R E_G(R))^{\Delta(\psi)}$ by $\tilde{S}_M$. By Lemma 3.6, $\tilde{S}_M$ is $\tilde{R}G$-isomorphic to $S_M \otimes_{RG} R\tilde{G}$. In particular, it is $R\tilde{G}$-projective. Therefore it has the form

$$\tilde{S}_M \cong \bigoplus_{N \in \mathfrak{A}(M)} S_N, \qquad \mathfrak{A} \subset \mathrm{Sim}(k,\tilde{G}).$$

We determine $\mathfrak{A}_M$. Reducing $\mathrm{mod}\,\pi$, we get

$$\begin{aligned} \tilde{S}_M/\pi\tilde{S}_M &= (S_M/\pi S_M) \otimes_{kG} k\tilde{G} \\ &= M \otimes_{kG} k\tilde{G} = \bigoplus_{\psi^{\#}(N)=M} . \end{aligned}$$

Therefore $\mathfrak{A}_M = (\psi^{\#})^{-1}(M)$. We start again with equation $(*)$:

$$\begin{aligned} \bigoplus_M \pi^{f(M)} \cdot (S_M \otimes E_{\tilde{G}}(R))^{\Delta(\psi)} &= \bigoplus_M \pi^{f(M)} \cdot \tilde{S}_M \\ &= \bigoplus_M \pi^{f(M)} \cdot \left(\bigoplus_{N \in \mathfrak{A}_M} S_N\right) \\ &= \bigoplus_N \pi f(\psi^{\#}(N)) S_N. \end{aligned}$$

Hence

$$\varphi(R, \tilde{G})(\mathrm{PO}(R, \psi)(A)) = \varphi(R, \tilde{G})\left(\bigoplus_N \pi f(\psi^{\#}(N)) \cdot S_N\right)$$
$$= f\psi^{\#} = \mathrm{Map}\left(\psi^{\#}, \frac{1}{n}\mathbf{Z}\right)(f)$$
$$= \mathrm{Map}\left(\psi^{\#}, \frac{1}{n}\mathbf{Z}\right)(\varphi(R, G)(A)), \quad \text{Q.E.D.}$$

Lemma 3.6. *For all RG-modules U, one has*

$$(U \otimes_R E_{\hat{G}}(R))^{\Delta(\psi)} \cong U \otimes_{RG} R\tilde{G}.$$

Proof. One verifies that the maps

$$\text{restriction of } (U \otimes \tau \mapsto U \otimes \tau) \text{ to } (U \otimes_R E_{\hat{G}}(R))^{\Delta(\Psi)},$$

$$\frac{1}{n}\sum_{\sigma \in G} \sigma u \otimes \psi(\sigma)^{-1}\tau \leftarrow u \otimes \tau,$$

are well defined and inverse isomorphisms.

We conclude this section with

Theorem 3.7. *The kernel* $\ker(\varphi(R, G))$ *consists precisely of the G-Galois extensions A of R.*

Comments. 1. A stands for the order (A, L), $L = K \otimes_R A$, as usual. 2. In particular, $\varphi(R, G)(A) = 0$ with A a *preorder* implies A is actually an order.

Proof. Write φ for $\varphi(R, G)$ and let A be a preorder. We must show:

$$\varphi(A) = 0 \Leftrightarrow A \text{ is a separable } R\text{-algebra}.$$

(Note that A is G-Galois over R iff it is a separable order in a G-Galois extension of K.)

$\Leftarrow$: $\varphi(A) = (1/n)\varphi_0 A^{*n}$ where $n = |G|$. A^{*n} is again a separable R-algebra since $*$ is the product in the abelian group $\mathrm{Gal}(R, G)$. Moreover, it is semitrivial. Since A^{*n} is integral over R, we have $A^{*n} \subset E_G(R)$. Since any morphism of G-Galois extensions is an isomorphism, $A^{*n} = E_G(R)$, and $\varphi_0(A^{*n})$ is the zero map by definition.

$\Leftarrow$: There exists an inclusion $t: R \to T$, T Dedekind, such that $T \otimes_R A = \mathrm{PO}(t, G)(A)$ is semitrivial (as in the end of the proof of 2.5). Since φ and $\mathrm{PO}(t, G)$ commute (Theorem 3.2), we also have

$$\varphi(T, G)(T \otimes A) = 0 = \varphi_0(T, G)(T \otimes A).$$

Thus $T \otimes A = E_G(T)$ by definition of φ_0, $T \otimes A/T$ is separable. Since T/R is faithfully flat, A/R is separable. Q.E.D.

4. The image of the group homomorphism φ

We resume the notation from 3.0. We defined

$$\varphi\colon \mathrm{TPO}(R, G) \to \mathrm{Map}(\mathrm{Sim}(k, G), (1/n)\mathbf{Z})$$

and calculated the kernel. For brevity, let $\mathrm{Sim}(k, G) = C = C_G$, $\varphi(R, G) = \varphi$. We summarize our knowledge of φ (and $\mathrm{TPO}(R, G)$) as follows:

Proposition 4.1. *There is an exact sequence*

$$0 \to \mathrm{Gal}(R, G) \underset{i}{\hookrightarrow} \mathrm{TPO}(R, G) \to \mathrm{Map}_0\left(C, \frac{1}{n}\mathbf{Z}\right).$$

Here $\mathrm{Map}_0(C, (1/n)\mathbf{Z})$ *is the set of all maps* $C \to (1/n)\mathbf{Z}$ *whose value on the trivial representation* $I \in C$ *is zero.*

Proof. The embedding i sends A to the preorder $(A, K \otimes_R A)$, which we also denote A. The exactness is just Theorem 3.7. We still must show $\mathrm{Im}(\varphi)$ is contained in Map_0. It is enough to check $f(I) = 0$ for $f = \varphi(A)$ and A semitrivial. We have $A = \bigoplus_{M \in C} \pi^{f(M)} \cdot S_M$, and from the definition of tame preorders it follows that $A^G = R \cdot 1$. One checks that $R \cdot 1 \subset E_G(R)$ coincides with $S_I \subset {}^{\oplus}E_G(R)$. Moreover, $A^G = \pi^{f(I)}\colon S_I$. Hence $R \cdot I \subset A$ implies $f(I) = 0$. Q.E.D.

Now let $\mathrm{TPO}_0(R, G)$ denote the subgroup of semitrivial tame preorders in $\mathrm{TPO}(R, G)$. There is a canonical group homomorphism

$$\alpha\colon \mathrm{TPO}(R, G) \to \mathrm{Gal}(K, G),$$

sending (A, L) to L (or sending A to $K \otimes_R A$).

Proposition 4.2. *There is a short exact sequence*

$$0 \to \mathrm{TPO}_0(R, G) \to \mathrm{TPO}(R, G) \xrightarrow{\alpha} T\,\mathrm{Gal}(K, G) \to 1,$$

where $T\,\mathrm{Gal}(k, G)$ *is the subgroup of all* G*-Galois extensions of the number field* K *which are tame in the classical sense.*

demo Proof $\mathrm{Ker}(\alpha) = \mathrm{TPO}_0(R, G)$ by definition. We have to show that L is (classically) tame for $(A, L) \in \mathrm{TPO}(R, G)$ and that all such L occur in this way. For the first statement consider $K \subset L^H \subset L$ (H is the non-p-part of G as usual). Since A^H is a separable R-algebra and an order in L^H, L^H is even unramified over K, hence tame. Since $(p, |H|) = 1$, L is automatically tame over L^H. Hence $L \mid K$ is tame. On the other hand, let $L \mid K$ be tame and take A to be its maximal order. We claim (A, L) is tame. By Theorem 2.3 it suffices to show that A is an invertible RG-module, i.e., A has a normal basis. But this follows from Noether's theorem on tameness and normal bases. Q.E.D.

Let $U\,\mathrm{Gal}(K, G) \subset T\,\mathrm{Gal}(K, G)$ be the subgroup of unramified G-Galois extensions of K. Consider the following commutative diagram (the map ψ is

defined by it):

$$\begin{array}{ccccccccc}
 & & & & 0 & & 0 & & \\
 & & & & \downarrow & \overset{\varphi_0}{\underset{\cong}{\rightarrow}} & \downarrow & & \\
 & & 0 & \rightarrow & \mathrm{TPO}_0(R,G) & & \mathrm{Map}_0(C,\mathbf{Z}) & \rightarrow & 0 \\
 & & \downarrow & & \cap & & \cap & & \\
0 & \rightarrow & \mathrm{Gal}(R,G) & \xrightarrow{i} & \mathrm{TPO}(R,G) & \xrightarrow{\varphi} & \mathrm{Map}_0\left(C,\tfrac{1}{n}\mathbf{Z}\right) & & \\
 & & \downarrow \cong & & \downarrow \alpha & & \downarrow p & & \\
0 & \rightarrow & U\,\mathrm{Gal}(K,G) & \subset & T\,\mathrm{Gal}(K,G) & \xrightarrow{\psi} & \mathrm{Map}_0\left(C,\tfrac{1}{n}\mathbf{Z}/\mathbf{Z}\right) & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array}$$

Proposition 4.3. *The above diagram is commutative and exact.*

Proof. It can be seen from the construction of φ_0 that it is an isomorphism onto $\mathrm{Map}_0(C,\mathbf{Z})$. The rest of the diagram is easily checked for exactness, except (maybe) at $T\,\mathrm{Gal}(K,G)$ in the bottom line. This requires a standard diagram chase.

Our objective is to analyze the group $\mathrm{TPO}(R,G)$. The following remarks explain why we need to understand $\mathrm{Im}(\varphi)$.

Remarks 4.4. (a) $\mathrm{TPO}(R,G) \cong \mathrm{Gal}(R,G) \oplus \mathrm{Im}(\varphi)$.

(b) If we take the other short exact sequence

$$0 \rightarrow \mathrm{TPO}_0(R,G) \rightarrow \mathrm{TPO}(R,G) \rightarrow T\,\mathrm{Gal}(K,G) \rightarrow 0,$$

we also get a description of $\mathrm{TPO}(R,G)$ by two quantities which are (in principle) known (see above diagram), but the sequence rarely splits. (One can show it splits iff $T\,\mathrm{Gal}(K,G) = U\,\mathrm{Gal}(K,G)$).

Proof of (a). Since $\mathrm{Im}(\varphi)$ is a subgroup of the free group $\mathrm{Map}(C,(1/n)\mathbf{Z})$, $\mathrm{Im}(\varphi)$ is free, hence the exact sequence given by 4.1 splits. From the diagram (4.3), it is clear that we only need to describe $\mathrm{Im}(\psi)$. Then we will also know $\mathrm{Im}(\varphi)$, since

$$\mathrm{Im}(\varphi) = p^{-1}(\mathrm{Im}(\psi))$$

(recall p was the projection $\mathrm{Map}_0(C,(1/n)\mathbf{Z}) \rightarrow \mathrm{Map}_0(C,(1/n)\mathbf{Z}/\mathbf{Z})$. In a special case, $\mathrm{Im}(\psi)$ has a nice description:

Theorem 4.5. *Suppose G is isomorphic to k^*. Then $C = (\mathrm{Sim}(k,G) =) \mathrm{Hom}(G,k^*)$ is an abelian group, and*

$$\mathrm{Im}(\psi) = \mathrm{Hom}(C,(1/n)\mathbf{Z}/\mathbf{Z}) \subset \mathrm{Map}_0(C,(1/n)\mathbf{Z}/\mathbf{Z}).$$

Proof. We need the following statements from local class field theory:

(1) $\mathrm{Gal}(K,G) \cong \mathrm{Hom}_c(K^*,G)$, and the isomorphism is given by the *norm residue symbol*. More precisely: if $L \in \mathrm{Gal}(K,G)$, then L corresponds to the element $f_L \in \mathrm{Hom}_c(K^*,G)$ which satisfies: $f_L(\alpha) \in G$ is the same automorphism of L as $(\alpha/(L/K))$.

(2) $L \in \mathrm{Gal}(K, G)$ is *tame* iff $f_L(U^{(1)}(K)) = 1$, where $U^{(1)}(K) = \{x \in R^* \mid x \equiv 1(\pi)\}$.

(3) $L \in \mathrm{Gal}(K, G)$ is *unramified* iff $f_L(R^*) = 1$. The structure of K^* is well known:

$$K^* = \pi^{\mathbf{Z}} \times U^{(1)}(K) \times \beta(k^*),$$

where $\beta: k^* \to K^*$ is the (!) multiplicative system of representatives. We suppress β in the notation.

From statements (2) and (3), we get a canonical isomorphism (using the above decomposition of K^*):

$$\mathrm{Hom}(\pi^{\mathbf{Z}} \times k^*, G) \xrightarrow[\cong]{} T\,\mathrm{Gal}(K, G),$$

$$\mathrm{Hom}(\pi^{\mathbf{Z}}, G) \xrightarrow[\cong]{} U\,\mathrm{Gal}(K, G).$$

Together, these induce a canonical isomorphism

$$\lambda: \mathrm{Hom}(k^*, G) \xrightarrow[\cong]{} T\,\mathrm{Gal}(R, G)/U\,\mathrm{Gal}(R, G).$$

The map ψ induces (see 4.3) a map

$$\overline{\psi}: T\,\mathrm{Gal}(R, G)/U\,\mathrm{Gal}(R, G) \hookrightarrow \mathrm{Map}_0(C, (1/n)\mathbf{Z}/\mathbf{Z}).$$

Now there is an explicitly described map E from the domain of λ to the range of $\overline{\psi}$ (recall $C = \mathrm{Hom}(G, k^*)$)

$$E: \mathrm{Hom}(k^*, G) \to \mathrm{Map}_0(\mathrm{Hom}(G, k^*), (1/n)\mathbf{Z}/\mathbf{Z})$$

with $E(\alpha)(\chi) = v/n + \mathbf{Z}$ where $\alpha_\chi = r - \mathrm{id}_G \in \mathrm{End}(G)$ (for $\alpha \in \mathrm{Hom}(k^*, G)$, $\chi \in \mathrm{Hom}(G, k^*)$). Keep in mind that we want to describe $\mathrm{Im}(\overline{\psi})$.

Main Lemma 4.6. $\overline{\psi}\lambda = -E$.

Proof of 4.6. Let $s: k^* \to G$ be an isomorphism. Since s generates $\mathrm{Hom}(k^*, G)$, it suffices to show $\psi\lambda(s) = -E(s)$. For this purpose, we need to know explicitly the quantity $\lambda(s)$, i.e., the tame G-extension L associated to s by class field theory, up to a factor in $U\,\mathrm{Gal}(k, G)$. So let us find L.

Let $q = |k^*|$. Recall π was a parameter of R. Define $L = K[\sqrt[q-1]{\pi}]$ with the following G-action:

$$g\left(\sqrt[q-1]{\pi}\right) = s^{-1}(g^{-1}) \cdot \sqrt[q-1]{\pi}.$$

(Note $s^{-1}(g^{-1})$ is in k^*, and since we identified k^* with a subgroup of K^*, $s^{-1}(g^{-1})$ is a $q-1$ st root of unity.) We claim $f_L = s$, i.e., $\lambda(s) = L \cdot U'\,\mathrm{Gal}(K, G)$. To check this, we need

Sublemma 4.7. *For $\alpha \in k^* \subset R^*$ we have*

$$(\alpha/(L/K))(\sqrt[q-1]{\pi}) = \alpha^{-1}\sqrt[q-1]{\pi}.$$

Proof. L is the Lubin-Tate extension L_F for the polynomial $F(x) = X^q - \pi X$. (See Neukirch [N, p. 163].) Then $(\alpha/(L/K)) = (\alpha^{-1})_F$ = the multiplication by α^{-1} on the Lubin-Tate module $\{x \mid x^q - \pi x = 0\} \subset L$ [N, p. 179]. Therefore

$$(*) \qquad (\alpha/(L/K))(\sqrt[q-1]{\pi}) \equiv \alpha^{-1}\sqrt[q-1]{\pi}(\sqrt[q-1]{\pi^2})$$

[N, p. 166].

On the other hand, $(\alpha/(L/K))(\sqrt[q-1]{\pi})$ is a $q-1$st root of π. Since α^{-1} is a $q-1$st root of 1, $(*)$ has to be an equality. Q.E.D. (4.7)

Now let $\alpha \in k^* \subset R^*$. Then $(\alpha/(L/K))\sqrt[q-1]{\pi} = \alpha^{-1}\sqrt[q-1]{\pi}$ by 4.7, and the latter equals $s(\alpha)(\sqrt[q-1]{\pi})$ by the definition of L and its G-structure. Hence $(\alpha/(L/K)) = s(\alpha)$. By statement (1), $(\alpha/(L/K)) = f_L(\alpha)$. Hence $f_L = s$ as claimed, and we have calculated $\lambda(s) = L \cdot U\,\mathrm{Gal}(K, G)$.

Now let us calculate $\psi(L)$. By definition, $\psi(L) = \varphi(A) + \mathbf{Z}$ for A any G-order in L. Take A to be $R[\sqrt[q-1]{\pi}] \cong R[X]|(X^{q-1} - \pi)$. Let $k^* \subset K^*$ be generated by ζ and $\sigma = s(\zeta)$. Then $\sigma(\overline{X}) = \zeta^{-1}\overline{X}$ by definition of L and its G-structure. In evaluating $\varphi(A)$, we use the recipe (Corollary 3.4)

$$\varphi(A) = (1/(q-1))\varphi_0(B)$$

with B the $q-1$st $*$-power of A. It is fairly easy to check that $B = A*\cdots*A \cong R[X]/(X^{q-1} - \pi^{q-1})$ with $\sigma(\overline{X}) = \zeta^{-1}\overline{X}$. Now B is subtrivial, and we explicitly have an injection j:

$$\begin{aligned} j\colon B &\to R \times \cdots \times R = E_R(G), \\ 1 &\to (1, \ldots, 1), \\ X &\to (\pi, \zeta\pi, \ldots, \zeta^{q-2}\pi), \\ &\vdots \\ X^{q-2} &\to (\pi^{q-2}, \zeta^{q-2}\pi^{q-2}, \ldots, \zeta^{(q-2)^2}\pi^{q-2}). \end{aligned}$$

γ is G-equivariant for σ operating as a right shift on $R \times \cdots \times R$. From this it follows that

$$\begin{aligned} \gamma(B) = &(\text{eigenspace of } \sigma \text{ to the eigenvalue } 1) \\ &\oplus \pi(\text{eigenspace of } \sigma \text{ to the e.v. } \zeta^{-1}) \\ &\oplus \pi^2(\text{eigenspace of } \sigma \text{ to the e.v. } \zeta^{-2}) \\ &\oplus \pi^{q-2}(\text{eigenspace of } \sigma \text{ to the e.v. } \zeta^{-q+2}). \end{aligned}$$

Now recall that we identified $C = \mathrm{Sim}(k, G)$ with $\mathrm{Hom}(G, k^*)$ (simple kG-modules correspond to characters $\chi\colon G \to k^*$). The complete list of characters is here $\chi_0, \chi_1, \ldots, \chi_{q-2}$ with $\chi_i(\sigma) = \zeta^i$. The eigenspace of σ to the eigenvalue ζ^i in $R \times \cdots \times R$ corresponds to a simple kG-module (via reduction mod π), namely the module k with σ operating as multiplication by ζ^j. This simple module belongs to the character χ_j. Using the definition of φ_0, we now

get that $\varphi_0(B)$ is the following map (still identifying $C = \mathrm{Sim}(k, G)$ with the character group $\mathrm{Hom}(G, k^*)$):

$$\begin{aligned} \chi_0 &\mapsto 0, \\ \chi_{-1} &\mapsto 1, \\ &\vdots \\ \chi_{-q+2} &\mapsto q-2. \end{aligned}$$

Hence $\varphi(A)$ is the map

$$\begin{aligned} \chi_0 &\mapsto 0, \\ \chi_1 &\mapsto -1/(q-1), \\ \chi_2 &\mapsto 2/(q-1), \\ &\vdots \\ \chi_{q-2} &\mapsto -(q-2)/(q-1), \end{aligned}$$

and $\psi(A) = \psi\lambda(s)$ is the same thing read modulo $\mathbf{Z}$. Now one looks up the definition of $E(s)$, uses that $n = |G| = |k^*| = q - |$, and gets the same outcome for $-E(s)$. Q.E.D. (4.6)

Now 4.5 is easy to prove: we have

$$\begin{aligned} \mathrm{Im}(\psi) &= \mathrm{Im}(\psi\lambda) \quad (\text{since } \lambda \text{ is an isomorphism}) \\ &= \mathrm{Im}(E) \quad \text{by the main lemma.} \end{aligned}$$

Recall E was a monoid homomorphism

$$\begin{aligned} E\colon \mathrm{Hom}(k^*, G) \quad &\to \quad \mathrm{Map}_0(C, (1/n)\mathbf{Z}/\mathbf{Z}) \\ &\qquad\qquad \| \\ &\qquad \mathrm{Map}_0(\mathrm{Hom}(G, k^*), (1/n)\mathbf{Z}/\mathbf{Z}). \end{aligned}$$

One can check that E is injective, and from the definition it follows easily that $\mathrm{Im}(E) \subset \mathrm{Hom}(C, (1/n)\mathbf{Z}/\mathbf{Z})$. Now $\mathrm{Hom}(k^*, G)$ and $\mathrm{Hom}(C, (1/n)\mathbf{Z}/\mathbf{Z})$ both have cardinality $q - 1 = n$, therefore $\mathrm{Im}(E) = \mathrm{Hom}(C, (1/n)\mathbf{Z}/\mathbf{Z})$. This finishes the proof of Theorem 4.5. Q.E.D.

Theorem 4.5 describes $\mathrm{Im}(\varphi)$ in the special case $G \cong k^*$. In the general case, we have a slightly less explicit description. From now on, we provide our maps φ, ψ, etc. with subscripts φ_G, ψ_G, etc. to make clear which group G is meant.

Theorem 4.8. *Let G be a finite abelian group, R, ψ_G as above. Let $G[q-1] = \{g \in G | g^{q-1}\} = e$, $j\colon G[q-1] \subset G$ the inclusion $(q - 1 = |k^*|)$. Then*

$$\begin{aligned} \mathrm{Im}(\psi G) &= \mathrm{Map}\left(j^{\#}, \frac{1}{q-1}\mathbf{Z}/\mathbf{Z}\right)(\mathrm{Im}(\psi_{G[q-1]})) \\ &= \mathrm{Map}\left(j^{\#}, \frac{1}{q-1}\mathbf{Z}/\mathbf{Z}\right)\left(\mathrm{Hom}\left(\mathrm{Sim}(k, G[q-1]), \frac{1}{q-1}\mathbf{Z}/\mathbf{Z}\right)\right). \end{aligned}$$

(*For the definition of $j^{\#}$, see* 3.5.)

Proof. Let us first consider the case $G = G[q-1]$. We have to show $\mathrm{Im}(\psi_G) = \mathrm{Hom}(C_G, (1/(q-1))\mathbf{Z}/\mathbf{Z})$. Let Γ be (a copy of) the finite abelian group k^* (we introduce the letter Γ for formal reasons). Let $\sigma \in \mathrm{Hom}(k^*, G)$. Consider the commutative diagram

$$\begin{array}{ccc} \mathrm{Hom}(k^*, \Gamma) & \xrightarrow{\overline{\psi_\Gamma}} & \mathrm{Hom}\left(C_\Gamma, \frac{1}{q-1}\mathbf{Z}/\mathbf{Z}\right) \\ {\scriptstyle \mathrm{Hom}(k^*, G)}\downarrow & & \downarrow {\scriptstyle \mathrm{Map}(\sigma^\#, \mathrm{id})} \\ \mathrm{Hom}(k^*, G) & \xrightarrow{\overline{\psi}_G} & \mathrm{Map}_0\left(C_G, \frac{1}{n}\mathbf{Z}/\mathbf{Z}\right). \end{array}$$

(The commutativity comes from 3.5 and the functionality of the reciprocity isomorphisms.)

Since $G = G[q-1]$, we may say $C_G = \mathrm{Hom}(G, K^*)$, and of course also $C_\Gamma = \mathrm{Hom}(\Gamma, K^*)$. Let us take $\mathrm{id} \in \mathrm{Hom}(k^*, \Gamma)$ and chase it the low road from top left to bottom right. We get $\overline{\psi}_G(\sigma)$. Since we could have chased it the high road, too, we get that $\overline{\psi}_G(\sigma) \in \mathrm{Im}(\mathrm{Map}(\sigma^\#, \mathrm{id})) \subset \mathrm{Hom}(C_G, (1/n)\mathbf{Z}/\mathbf{Z})$; i.e., we may redraw our diagram (in doing so, we extend it to the right):

$$\begin{array}{ccccc} \mathrm{Hom}(k^*, \Gamma) & \xrightarrow{\psi_\Gamma} & \mathrm{Hom}\left(\mathrm{Hom}(\Gamma, k^*), \frac{1}{q-1}\mathbf{Z}/\mathbf{Z}\right) & \overset{h}{\cong} & \Gamma \\ {\scriptstyle \mathrm{Hom}(k^*, \sigma)}\downarrow & & \downarrow & {\scriptstyle \mathrm{Hom}(\mathrm{Hom}(\sigma, k^*), \mathrm{id})}\downarrow\sigma & \\ \mathrm{Hom}(k^*, G) & \xrightarrow{\psi_G} & \mathrm{Hom}\left(\mathrm{Hom}(G, k^*), \frac{1}{q-1}\mathbf{Z}/\mathbf{Z}\right) & \cong & \Gamma. \end{array}$$

h is a canonical isomorphism gotten by selecting any generator of k^*. We claim: ψ_G is subjective (this proves 4.8 for $G = G[q-1]$).

Take $x \in \mathrm{Hom}(\mathrm{Hom}(G, k^*), (1/(q-1))\mathbf{Z}/\mathbf{Z})$. Then $h(x) \in G$, and there exists some σ with $h(x) \in \mathrm{Im}(\sigma)$; i.e., $h(x) = \sigma(\gamma)$ with $\gamma \in \Gamma$. Take a preimage y of γ under $h\overline{\psi}_G$. Chasing the diagram, one sees that $z = \mathrm{Hom}(k^*, \sigma)(y)$ is a preimage y of γ under $h\overline{\psi}_G$. Chasing the diagram, one sees that $z = \mathrm{Hom}(k^*, \sigma)(y)$ is a preimage of x under $\overline{\psi}_G$.

The proof in the general case is a formal consequence. Consider γ: $G[q-1] \hookrightarrow G$ and the diagram

$$\begin{array}{ccc} \mathrm{Hom}(k^*, G[q-1]) & \xrightarrow{\overline{\psi}_{G[q-1]}} & \mathrm{Hom}\left(C_{G[q-1]}, \frac{1}{q-1}\mathbf{Z}/\mathbf{Z}\right) \\ {\scriptstyle \mathrm{Hom}(k^*, j)}\downarrow & & \downarrow {\scriptstyle \mathrm{Map}\left(j^\#, \frac{1}{q-1}, \mathbf{Z}/\mathbf{Z}\right)} \\ \mathrm{Hom}(k^*, G) & \xrightarrow{\psi_G} & \mathrm{Map}_0\left(C_G, \frac{1}{n}\mathbf{Z}/\mathbf{Z}\right). \end{array}$$

As above, the diagram commutes. The left vertical arrow is onto since $|k^*| = q-1$. Therefore $\mathrm{Im}(\psi G)$ equals $\mathrm{Map}(j^\#, (1/(q-1))\mathbf{Z}/\mathbf{Z})(\mathrm{Im}(\psi_{G[q-1]}))$. This proves the theorem, since we know from the first part that $\psi_{G[q-1]}$ is onto

$$\mathrm{Hom}(C_{G[q-1]}, (1/(q-1))\mathbf{Z}/\mathbf{Z}).$$

Examples 4.9. (a) Take $G = C_3$, R a complete number ring with $\mathrm{char}(k) \neq 3$, $\zeta_3 \in k^*$. (Take a completion of $\mathbf{Z}[\zeta_3]$ at any prime not dividing 3.) Then $C = \mathrm{Sim}(k, G)$ is a three-element group $\langle c_0, c_1, c_2 \rangle$ (c_0 = neutral element=trivial

representation). Then

$$\mathrm{Im}(\psi) = \mathrm{Hom}(C, \tfrac{1}{3}\mathbf{Z}/\mathbf{Z}),$$
$$\mathrm{Im}(\varphi) = \{f: C \to \tfrac{1}{3}\mathbf{Z} \mid f(c_0) = 0,\ f(c_2) \equiv 2 \cdot f(c_1)(\mathbf{Z})\}.$$

Recall that $\mathrm{TPO}(R, G)$ is the middle term of a short exact sequence

$$0 \to \mathrm{Gal}(R, G) \to \mathrm{TPO}(R, G) \to \mathrm{Im}(\varphi) \to 0.$$

$\mathrm{Gal}(R, G)$ can be calculated by Kummer theory or local class field theory. Moreover, as noted before, the sequence splits.

(b) Take the same setting, but $\zeta_3 \notin k^*$. This means $G[q-1]$ is trivial (3 does not divide $|k^*| = q - 1$). By Theorem 4.8, $\mathrm{Im}(\overline{\psi}_G)$ has but one element. Therefore

$$\mathrm{Im}(\varphi) = \mathrm{Map}_0(C, \mathbf{Z}),$$

and $C = \{c_0, c_1\}$, c_1 the only nontrivial representation.

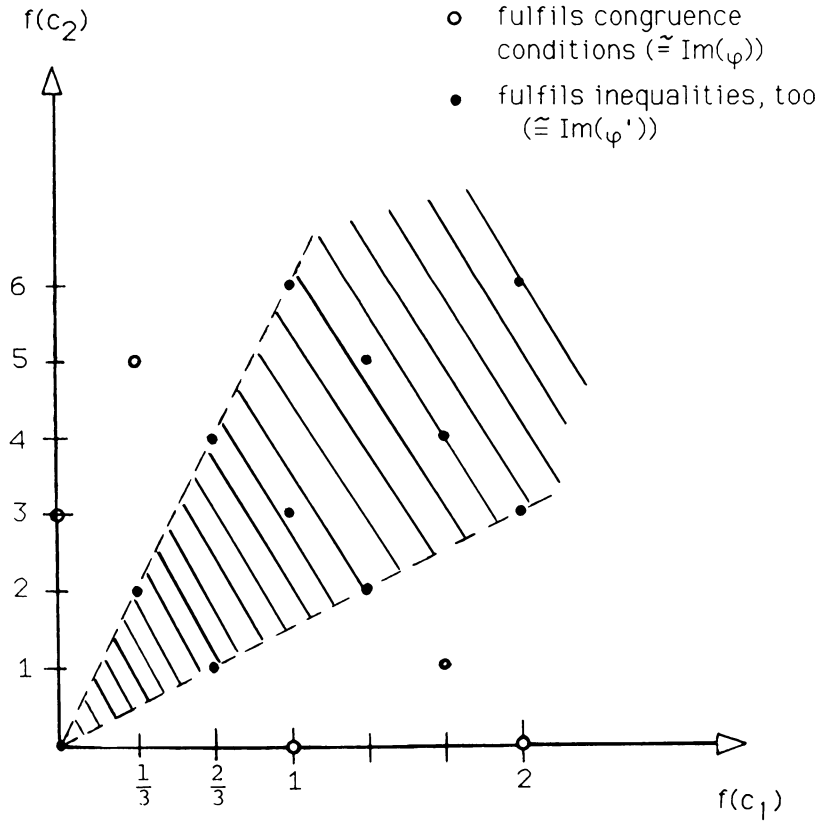

FIGURE 1

5. The image of (φ restricted to orders)

The main object of investigation is the monoid $\mathrm{TO}(R, G)$ of tame orders (notation of the preceding sections). Preorders were brought into play mainly in order to have a sensible way of embedding TO into an abelian group. Let

$$\varphi' \colon \mathrm{TO}(R, G) \to \mathrm{Map}_0(C, (1/n)\mathbf{Z}/\mathbf{Z})$$

be the restriction of φ from TPO to TO. What can be said about $\mathrm{Im}(\varphi')$?

Roughly speaking, the outcome is this: while the image of φ itself is determined by congruence conditions $\bmod \mathbf{Z}$ for maps $f\colon C \to (1/n)\mathbf{Z}$ (to int: $f \bmod \mathbf{Z}$ a homomorphism), the image of φ' is defined by an additional set of inequalities among the values of $f\colon C \to (1/n)\mathbf{Z}$.

Example 5.1 (cf. 4.9). $G = C_3$ and $\zeta_3 \in k^*$. We wrote $C = \{c_0, c_1, c_2\}$, and we showed

$$\mathrm{Im}(\varphi) = \{f\colon C \to \tfrac{1}{3}\mathbf{Z} \mid f(c_0) = 0,\ f(c_2) \equiv 2f(c_1) \bmod \mathbf{Z}\}.$$

We shall prove that (in this case)

$$\mathrm{Im}(\varphi') = \{f \in \mathrm{Im}(\varphi) \mid 0 \le f(c_2) \le 2f(c_1),\ 0 \le f(c_1) \le 2f(c_2)\}.$$

This gives a fairly explicit description of $\mathrm{TO}(R, G)$ as a monoid. We know generally that $\varphi\colon \mathrm{TPO}(R, G) \to \mathrm{Im}(\varphi)$ is a split epi (4.4a). Since $\ker(\varphi) \subset \mathrm{TO}(R, G)$ (Theorem 3.7), $\varphi'\colon \mathrm{TO}(R, G) \to \mathrm{Im}(\varphi')$ is a split surjection of monoids (the same splitting will do), hence

$$\begin{aligned}\mathrm{TO}(R, G) &\cong \mathrm{Ker}(\varphi) \oplus \varphi(\mathrm{TO}(R, G)) \\ &= \mathrm{Gal}(R, G) \oplus \mathrm{Im}(\varphi').\end{aligned}$$

In Examples 5.1, $\mathrm{Im}(\varphi^1)$ can be visualized as in Figure 1. All $f \in \mathrm{Im}(\varphi)$ are given by $f(c_1)$ and $f(c_2)$, since $f(c_0) = 0$ anyway.

In order to state the theorem, we have to fix notation and give a definition. Let R be a *DVR* with residue class field k, G a finite abelian group, H its non-p part where $p = \mathrm{char}(k)$, and $C = \mathrm{Sim}(k, H) \cong \mathrm{Sim}(k, G)$ the set of simple kG-modules up to isomorphism.

Definition 5.2. We define a ternary relation $(-,-)\ \mathrm{rel}(-)$ on C as follows. Let $M, N, P \in C$. Then $(M, N)\,\mathrm{rel}\,P$ if ${}_{kG}P$ is a direct summand of $M \otimes_k N$. (As usual, G operates diagonally on $M \otimes_R N$.)

Example. Suppose kG splits, and M, N belong to (one-dimensional) characters χ_M and χ_N. Then $M \otimes N$ belongs to the character $\chi_M \cdot \chi_N$, and hence

$$(M, N)\,\mathrm{rel}\,P \Leftrightarrow \chi_P = \chi_M \cdot \chi_N.$$

(One may visualize "rel" as a "product of irreducible representations with probabilistic outcome" in general.)

Theorem 5.3. *Let* $(A, L) \in \mathrm{TPO}(R, G)$. *Then* A *is an algebra (i.e.,* $A \cdot A \subset A$*) if the following holds for* $f = \varphi(A)\colon C \to (1/n)\mathbf{Z}$:

$(*)$ $\quad f(P) \leq f(M) + f(N)$ *for all* (M, N, P) *with* $(M, N)\,\mathrm{rel}\,P$.

Let us say f *is admissible if* $(*)$ *holds.*

Remark. The set of admissible f is obviously a submonoid of the abelian group $\mathrm{Map}_0(C, (1/n)\mathbf{Z})$.

Proof. (1) Reduction to the semitrivial case. Let S/R be a faithfully flat extension, S a *DVR*, such that $S \otimes_R A$ is semitrivial over S (see the end of the proof of 2.5). Obviously, $S \otimes_R A$ is an algebra iff A is, and the same goes for A^{*n} in the place of A. We have the equivalences

$S \otimes_R A$ is an algebra

$\Leftrightarrow \varphi_S(S \otimes_R A)$ admissible (Theorem valid in semitrivial case; see (2) below)

$\Leftrightarrow n \cdot \varphi_S(S \otimes_R A)$ admissible (obvious from the definition)

$\Leftrightarrow S \otimes A^{*n}$ is an algebra.

By descent, A is an algebra iff A^{*n} is. Now we get:

A is an algebra

$\Leftrightarrow A^{*n}$ is an algebra

$\Leftrightarrow \varphi_R(A^{*n}) = n\varphi_R(A)$ admissible (A^{*n} is semitrivial, see (2) below)

$\Leftrightarrow \varphi_R$ admissible (obvious from definition).

(2) Proof in the semitrivial case: Let $A \in \mathrm{TPO}(R, G)$ be semitrivial. By tameness (Lemma 2.6) we have

$$A = E_{Gp}(A_0), \qquad A_0 \in \mathrm{TPO}(R, H).$$

Obviously A is an algebra iff A_0 is, and $\varphi(A) = \varphi(A_0)$ by construction. Therefore we may assume $G = H$. We have

$$E_G(R) = \bigoplus_{M \in C} S_M \quad \text{with } S_M \mid \pi S_M \cong M \text{ as } kG\text{-modules}.$$

Moreover, $A = \bigoplus_{M \in C} \pi^{f(M)} \cdot S_M$, $f = \varphi(A)$.

Lemma 5.4. *For all* $M, N \in C$ *we have*

$$S_M \cdot S_N = \bigoplus_{(M,N)\,\mathrm{rel}\,P} S_P \quad (\cdot \text{ denotes product inside } E_G(R)).$$

We postpone the proof of 5.4 and continue with the proof of 5.3. We proved in 4.1 that $1 \in A$ (this uses tameness). Suppose $A \cdot A \subset A$. This implies $(\pi^{f(M)} \cdot S_M)\ (\pi^{f(N)} \cdot S_N)$ is contained in A. By Lemma 5.4, this is equivalent to

$$\bigoplus_{(M,N)\,\mathrm{rel}\,P} \pi^{f(M)+f(N)} S_P \subset \bigoplus_P \pi^{f(P)} \cdot S_P = A.$$

But we have generally

$$\bigoplus_P \pi^{G(P)} S_P \subset \bigoplus_P \pi^{h(P)} S_P \Leftrightarrow \forall P(g(P) \geq h(P)).$$

($\Leftarrow$ is trivial, and $\Rightarrow$ follows from $\pi^{-1} S_P \subset S_P$.) Thus we get $f(M)+f(N) \geq f(P)$ for all P with $(M, N)\,\mathrm{rel}\,P$. The reverse implication of the theorem is proved in the same way.

Proof of 5.4. (a) Let us assume G splits over R (i.e., $\zeta_m \in R$ where $m = \exp(G)$). Then

$$S_M = R \cdot (\chi_M^{-1}(g))g \in G \subset E_G(R),$$
$$S_N = R \cdot (\chi_N^{-1}(g))g \in G \subset E_G(R), \quad \text{and}$$
$$S_M \cdot S_N = R \cdot (\chi_M^{-1}(g)\chi_N^{-1}(g))_{g \in G} = R \cdot (\chi_{M \otimes N}^{-1}(g))g \in G.$$

This gives the conclusion, since $(M, N)\,\mathrm{rel}\,P$ iff $P \equiv M \otimes N$ (see example following 5.2).

(b) Let us extend the definition of $(M, N)\,\mathrm{rel}\,P$ verbatim to M, N not necessarily simple (=indecomposable) and still assume G splits over R. Then the conclusion $S_M \cdot S_N = \bigoplus_{(M,N)\,\mathrm{rel}\,P} S_P$ obviously remains valid. Note in particular that $S_M \cdot S_N$ is a direct summand of $E_G(R)$.

(c) Now we do not assume G is split over R. By descent and using (b), $S_M \cdot S_N$ is a direct $R-G$ summand of $E_G(R)$. Therefore it has the form

$$S_M \cdot S_N = \bigoplus_{Q \in U} S_Q \quad \text{for some } U \subset C.$$

Reducing $\mathrm{mod}\,\pi$ gives

$$M \cdot N = \bigoplus_{Q \in U} Q \quad (\cdot \text{ denoting the product inside } E_G(k)).$$

We have $M \otimes_k N \twoheadrightarrow M \cdot N$, whence $M \cdot N \subset^{\oplus} M \otimes N$ since kG is semisimple. Therefore every $Q \in U$ satisfies $(M, N)\,\mathrm{rel}\,Q$. We also want to show the converse, i.e., the implication

$$Q \subset^{\oplus} M \otimes N \Rightarrow Q \subset^{\oplus} M \cdot N.$$

This claim is true if kG splits (write M and N as direct sums of one-dimensional representations).

Just suppose $Q \subset^{\oplus} M \otimes N$ but not $Q \subset^{\oplus} M \cdot N$. Let $l \supset k$ split G and denote $l \otimes k$ by a prime $'$. Then $Q' = \oplus Q_i$ with Q_i simple over lG, and all $Q_i \subset^{\otimes} (M \otimes N)'$, hence all $Q_i \subset^{\oplus} M' \cdot N'$. But $M \cdot N$ is nonzero and by assumption a direct sum of simple summands T_i nonisomorphic to Q. Since lG is a direct sum of pairwise nonisomorphic simple summands, no summand of any T_i' can be isomorphic to any Q_G. This is a contradiction. Q.E.D.

Remark 5.5. If $f \in \mathrm{Im}(\varphi)$ is admissible, it has only nonnegative values. This can be shown by hand but is also clear from the fact that tame orders are integral over R.

Example (5.1 revisited). (a) $G = C_3$, $\zeta_3 \in k$, $C = \{c_0, c_1, c_2\}$ as above. c_1 and c_2 are the two nontrivial representations (=characters), and

$$(*) \qquad (c_1, c_1) \operatorname{rel} c_2, \quad (c_2, c_1) \operatorname{rel} c_1.$$

The other relations involve c_0 (e.g., $(c_1, c_2) \operatorname{rel} c_0$). Since $f(c_0) = 0$ is known, the only information from them is

(1) $f(c_1) + f(c_2) \geq 0$.

From $(*)$ we get for $f \in \operatorname{Im}(\varphi^1)$.

(2) $f(c_2) \leq 2f(c_1)$, $f(c_1) \leq 2f(c_2)$.

By an elementary argument, (1) and (2) together are equivalent to

(3) $0 \leq f(c_2) \leq 2f(c_1)$, $0 \leq f(c_1) \leq 2f(c_2)$,

and this is the result announced in 5.1.

(b) Take the same example, but his time suppose $\zeta_3 \notin k$ (still $\operatorname{char}(k) \neq 3$). Now $C = \{c_0, c_1\}$, c_1 the only nontrivial representation of G over k. One computes that

$$(c_1, c_1) \operatorname{rel} c_0, \qquad (c_1, c_1) \operatorname{rel} c_1$$

(plus the obvious relation $(c_0, c_1) \operatorname{rel} c_1$). For $f \in \operatorname{Im}(\varphi)$, one gets here: f is admissible iff $f(c_1) \geq 0$. Since $\operatorname{Im}(\varphi) = \{f: C \to \mathbf{Z} \mid f(c_0) = 0\}$, we get

$$\operatorname{Im}(\varphi') = \{f: C \to \mathbf{Z} \mid f(c_0) = 0,\ f(c_1) \geq 0\}.$$

References

[CHR] S. Chase, D. K. Harrison and A. Rosenberg, *Galois theory and Galois cohomology of commutative rings*, Mem. Amer. Math. Soc., no. 52, 1965, pp. 15–33.

[CH] L. N. Childs and S. Hurley, *Local normal bases for objects of finite commutative, cocommutative Hopf algebras*, Trans. Amer. Math. Soc. (to appear).

[H] D. K. Harrison, *Abelian extensions of commutative rings*, Mem. Amer. Math. Soc., no. 52, 1965, pp. 1–14.

[N] J. Neukirch, *Klassenkorpertheorie*, Bibliographisches Institut, Mannheim, 1969.

Mathematische Institut, Universität München, D-8000 München 2, Federal Republic of Germany

Department of Mathematics, University of Oregon, Eugene, Oregon 97403