PACIFIC JOURNAL OF MATHEMATICS
Vol. 138, No. 1, 1989

ON CONSTRUCTIONS SIMILAR TO THE BURNSIDE RING FOR COMMUTATIVE RINGS AND PROFINITE GROUPS

C. GREITHER AND D. K. HARRISON

The question of finding all isomorphism classes of finite dimensional commutative semisimple rational algebras is an unsolved one and is equivalent to the question of finding all number fields. We feel that this problem may eventually be solved by the Burnside ring method, where the number fields are related to each other in many different ways. In this note we generalize the problem to the larger setting of G-algebras, where G is a finite abelian group. This gives even more relations—which we investigate. In order to see what is special about the rationals, we work as long as possible with a commutative ring R.

Separable ring extensions of a commutative ring R correspond by Galois theory to actions of a profinite group Γ. Hence we work with either commutative rings or profinite groups. In either case, we use a "twisting" by a finite abelian group G (more specifically, G cyclic of prime order). This allows us to form what we call the $*$-product. In the ring case, the $*$-product of R-algebras A and B is the R-algebra

$$A *_G B = \Big\{\sum x_i \otimes y_i \in A \otimes_R B \mid \sum x_i \otimes y_i = \sum \sigma x_i \otimes \sigma^{-1} y_i \ \forall \sigma \in G\Big\}.$$

One more parameter J is needed to get additive inverses in the resulting commutative ring with identity. (The addition comes from direct product in the ring case and from disjoint union in the case of sets with action of the profinite group.) In the ring case, we call the resulting ring $W(R, G; J)$. For k a finite field and G cyclic of order p, we calculate $W(R, G; J)$ explicitly.

1. General theory. Let R be a commutative ring which is nonzero (i.e. $1 \neq 0$) and which has no idempotents except 0 and 1. Let G be a finite abelian group. By an *(R, G)-algebra* (A, θ) we will mean a commutative, finitely generated, projective, separable R-algebra A with a group homomorphism θ from G to $\operatorname{Aut}_R(A)$. Let (A, θ) and

(B, Ψ) be such. We write

$$(A, \theta) \cong (B, \Psi)$$

if there exists an R-algebra isomorphism $f\colon A \to B$ such that

$$f \circ \theta(g) = \Psi(g) \circ f \quad \text{for all } g \in G.$$

$(A, \theta) *_G (B, \Psi)$ (or $A *_G B$ for short) will denote the pair

$$(\{u \in A \otimes_R B \mid (\theta(g) \otimes 1)(u) = (1 \otimes \Psi(g))(u)\ \forall g \in G\}, \theta \otimes 1).$$

This is again an (R, G)-algebra. $(A, \theta) \oplus (B, \Psi)$ (or $A \oplus B$ for short) will denote the pair

$$(A \times B, \theta \times \Psi).$$

Let (E, ε) denote the pair

$$(\mathrm{Map}(G, R), \varepsilon), \quad \varepsilon(g)(f) : h \to f(g^{-1}h).$$

Let us write $P(R, G)$ for the set of isomorphism classes of (R, G)-algebras. (The set-theoretical difficulties here can easily be overcome.)

THEOREM 1.1. *$\oplus$ and $*$ $(= *_G)$ induce on $P(R, G)$ the structure of a commutative semiring with additive cancellation and with neutral element (E, ε) of $*$.*

The *proof* of this and the following theorems will be given after Theorem 1.5 in a different setting. (A, θ) will be called *indecomposable* if $A \neq 0$, and

$$(A, \theta) \cong (X, \Psi_1) \oplus (Y, \Psi_2)$$

implies either $X = 0$ or $Y = 0$.

THEOREM 1.2. *Every (R, G)-algebra is a direct sum $(\oplus)$ of indecomposable ones in a unique way.*

Now let K be an abelian extension of R. For a definition, see **[2]**. If R is a number field, K is just an abelian field extension of R. We called (A, θ) *K-invertible* if there exists (B, Ψ) with

$$(A, \theta) *_G (B, \Psi) = (E, \varepsilon)$$

and

$$(K \otimes_R A, K \otimes \theta) \cong_K (K \otimes_R E, K \otimes \varepsilon),$$

where $\cong_K$ means isomorphism of (K, G)-algebras.

THEOREM 1.3. *The isomorphism classes of K-invertible (R,G)-algebras are finite in number. Under *, they form an abelian group $U_K(R,G)$ which is naturally isomorphic to* $\operatorname{Hom}(\operatorname{Aut}_R(K),G)$.

We call an (R,G)-algebra (A,θ) *K-hyperbolic* if

$$(A,\theta)*(B,\Psi)\cong(A,\theta)\quad\text{for all }(B,\Psi)\in U_K(R,G).$$

We call (A,θ) *K-reduced* if

$$(A,\theta)=(X,\Psi_1)\oplus(Y,\Psi_2),\quad (X,\Psi_1)\ K\text{-hyperbolic implies } X=0.$$

We denote the set of all (isomorphism classes of) K-reduced (R,G)-algebras by $W(R,G;K)$.

THEOREM 1.4. *Every (R,G)-algebra (A,θ) can be written uniquely in the form*

$$(A,\theta)=(A,\theta)_r\oplus(A,\theta)_h,$$

where $(A,\theta)_r\in W(R,G;K)$ and $(A,\theta)_h$ is K-hyperbolic.

Let $x,y\in W(R,G;K)$. Define

$$x+y=(x\oplus y)_r,$$
$$x\cdot y=(x*y)_r.$$

THEOREM 1.5. *With $+$ and $\cdot$, $W(R,G;K)$ is a commutative ring.*

Let $\overline{R}$ be the separable closure of R (see [3]) and let $\Gamma=\operatorname{Aut}_R(\overline{R})$ be the profinite Galois group of $\overline{R}$ over R. Let Alg_R denote the category of all commutative finitely generated, projective, separable R-algebras. Let Set_Γ denote the category of all finite continuous Γ-sets. (A Γ-set X is *continuous* if the stabilizer subgroup of every $x\in X$ is open in Γ.)

The functors

$$A\mapsto \mathrm{Alg}_R(A,\overline{R})\quad(A\in\mathrm{Alg}_R),$$
$$X\mapsto \mathrm{Set}_\Gamma(X,\overline{R})\quad(X\in\mathrm{Set}_\Gamma)$$

are (essentially) inverses of each other and establish a duality (= contravariant equivalence) of categories between Alg_R and Set_Γ (see [3] or [1]). A group homomorphism $G\to\operatorname{Aut}_R(A)$ will correspond to a group homomorphism

$$G\to\operatorname{Aut}_\Gamma(\mathrm{Alg}(A,\overline{R}))^{\mathrm{opp}}\cong\operatorname{Aut}_R(A).$$

Hence we have a contravariant equivalence of categories

$$\mathrm{Alg}_{(R,G)} \cong \mathrm{Set}_{(\Gamma,G)}\,.$$

The latter category (in which we choose to work) is described as follows:

Γ is a profinite group; G is a finite abelian group. A (Γ, G)-*biset* is a finite continuous $(\Gamma\times G)$-set. Equivalently, it is a triple (X, μ, ν) where

(i) X is a finite set.
(ii) $\mu\colon \Gamma\times X \to X$ is a continuous map, and
$\mu(\alpha, \mu(\beta, x)) = \mu(\alpha\beta, x)$, $\mu(e_\Gamma, x) = x$.
(iii) $\nu\colon G\times X \to X$ is a map, and
$\nu(\sigma, \nu(\tau, x)) = \nu(\sigma\tau, x)$, $\nu(e_G, x) = x$.
(iv) $\mu(\alpha, \nu(\sigma, x)) = \nu(\sigma, \mu(\alpha, x))\ \forall\alpha\in\Gamma\ \forall\sigma\in G$.

From now on, we write αx for $\mu(\alpha, x)$ and σx for $\nu(\sigma, x)$. An *example* is provided by G itself with the obvious G-action, and $\alpha x = x$ for $\alpha\in\Gamma$, $x\in G$.

Let X, Y be (Γ, G)-bisets. Write for $(x, y)\in X\times Y$:

$$\begin{gathered} x * y = \{(\sigma x, \sigma^{-1}y) \mid \sigma\in G\} \subset X\times Y; \\ X *_G Y = \{x * y \mid x\in X, y\in Y\}; \\ \sigma(x * y) = \sigma x * y\ (= x * \sigma y); \\ \alpha(x * y) = \alpha x * \alpha y. \end{gathered}$$

One checks that $X *_G Y$ is a well-defined (Γ, G)-biset. We write $X\oplus Y$ for the disjoint union $X \dot\cup Y$. In a canonical fashion, $X\oplus Y$ is again a (Γ, G)-biset. Let $P(\Gamma, G)$ denote the set of all isomorphism classes of (Γ, G)-bisets.

THEOREM 1.6. *For Γ a profinite group and G a finite abelian group, $\oplus$ and $*_G$ induce on $P(\Gamma, G)$ the structure of a commutative semiring with additive cancellation.*

Proof. All statements except the last one can be checked easily. The additive cancellation property follows from the fact that every $\Gamma\times G$-set has a unique decomposition as a disjoint union of transitive $\Gamma\times G$-sets (= orbits). For reference, let us point out this fact as a theorem:

THEOREM 1.7. *Every (Γ, G)-biset is uniquely the disjoint union of indecomposable ones.*

For $f \in \mathrm{Hom}_c(\Gamma, G)$, write G_f for the (Γ, G)-biset G with

$$\mu(\alpha, \sigma) = f(\alpha) \cdot \sigma, \quad \nu(\tau, \sigma) = \tau\sigma \quad (\sigma, \tau \in G,\ \alpha \in \Gamma).$$

One can check that $G_f * G_f = G_{f \cdot f}$, and G_1 is neutral in $P(\Gamma, G)$ under $*_G$.

THEOREM 1.8. *The units of $P(\Gamma, G)$ are exactly the bisets G_f, $f \in \mathrm{Hom}_c(\Gamma, G)$.*

Proof. Let $X *_G Y$ be isomorphic to G, via φ. Then $Y \neq \emptyset$, so take $y \in Y$. Let $x_1, x_2 \in X$. Since G_1 is transitive under G, there is $\sigma \in G$ such that

$$x_1 * y = \sigma(x_2 * y).$$

Hence there is a $\tau \in G$ such that $(x_1, y) = (\tau\sigma x_2, \tau^{-1} y)$. Therefore $x_1 = \tau\sigma x_2$, so G is transitive on X. Suppose $\sigma x = x$. Then $\sigma(x * y) = x * y$, so $\sigma = e_G$. Now choose $x_0 \in X$. For each $\alpha \in \Gamma$ there is exactly one $f(\alpha) \in G$ such that

$$\alpha x_0 = f(\alpha) x_0.$$

One checks that f is a homomorphism. $\mathrm{Ker}(f)$ is the stabilizer of x_0 in Γ, so it is open in Γ, and f is continuous. We have $G_f \cong X$ by $\sigma \mapsto \sigma x_0$. On the other hand, G_f is a unit with inverse G_f, $f(\alpha) = (f(\alpha))^{-1}$. This proves the theorem.

By a (Γ, G)-*triple* (or just *triple*) we mean a triple (Δ, H, t) where Δ is an open subgroup of Γ, H is a subgroup of G, and

$$t \colon \Delta \to G/H$$

is a continuous group homomorphism. For $\alpha \in \Gamma$, $(\alpha^{-1}\Delta\alpha, H, t^\alpha)$ is again a (Γ, G)-triple, where

$$t^\alpha(\delta) = t(\alpha\delta\alpha^{-1}).$$

We call this a *conjugate* of (Δ, H, t). Now let X be an indecomposable (Γ, G)-biset. Choose $x \in X$. Let

$$\begin{aligned} \Delta &= \{\delta \in \Gamma \mid \exists \sigma \in G \colon \delta x = \sigma x\}, \\ H &= \{\tau \in G \mid \tau x = x\}, \\ t(\delta) &= \sigma H \quad \text{if } \delta x = \sigma x. \end{aligned}$$

We call this the (Γ, G)-triple *associated* to X. One checks that

$$(\Delta, H, f \cdot t)$$

is the triple associated to $X *_G G_f$, where

$$(f \cdot t)(\delta) = f(\delta) t(\delta) \in G/H.$$

THEOREM 1.9. *The above correspondence sets up a bijection between the set of all isomorphism classes of indecomposable* (Γ, G)*-bisets and the set of all conjugacy classes of* (Γ, G)*-triples.*

Proof. The indecomposable (Γ, G)-bisets correspond to transitive continuous $\Gamma \times G$-sets, and these in turn correspond to conjugacy classes of open subgroups of $\Gamma \times G$. It is easily checked (and to our knowledge, a part of the mathematical folklore) that open subgroups of $\Gamma \times G$ can be described by triples as indicated above.

Now let J be a finite subgroup of $\mathrm{Hom}_c(\Gamma, G)$. For X a (Γ, G)-biset and $f \in J$, we write X_f for X with the new (Γ, G)-structure

$$\mu(\alpha, x) = f(\alpha) \cdot \alpha \cdot x, \qquad \nu(\sigma, x) = \sigma x.$$

Note that $X_f \cong X *_G G_f$. If $X = X_1 \oplus \cdots \oplus X_m, X_i$ indecomposable, then

$$X_f = (X_1)_f \oplus \cdots \oplus (X_m)_f,$$

and the $(X_i)_f$ are indecomposable. Call X *J-hyperbolic* if

$$X_f = X \quad \text{for all } f \in J.$$

Call X *J-reduced* if there is no J-hyperbolic $Z \neq \varnothing$ such that $X = Y \oplus Z$.

THEOREM 1.10. *Every biset X can be uniquely written as*

$$X = X_r \oplus X_h$$

with X_r J-reduced and X_h J-hyperbolic.

Proof. The only thing to prove is uniqueness. Hence suppose $X = Y \oplus Z$, Y J-reduced, Z J-hyperbolic. We proceed by induction over $|Z|$. If $Z = \varnothing$, $X = Y$ is J-reduced, so $X_h = \varnothing$, and we are done. Now suppose $\varnothing \neq Z = Z_1 \dot\cup \cdots \dot\cup Z_m$, Z_i indecomposable. Call Z_i *associate* of Z_1 if $Z_i \cong (Z_1)_f$ for some $f \in J$. Let $\tilde{Z} \subset Z$ be the disjoint union of all associates of Z_1, and $Z = \tilde{Z} \dot\cup W$. It is easily checked that both $\tilde{Z}$ and W are J-hyperbolic. Not all indecomposable pieces of $\tilde{Z}$ can lie in X_r, since X_r is reduced and $\tilde{Z} \neq \varnothing$. Therefore, without loss of generality, $Z_1 \subset X_h$. Since X_h is also hyperbolic, all associates of Z_1 are in X_h, too. Hence $\tilde{Z} \subset X_h$. Now we may cancel $\tilde{Z}$ from both representations $X = X_r \oplus X_h$, $X = Y \oplus Z$, and we get $X_r = Y$ and $X_h = Z$ from the induction hypothesis.

We write

$$W(\Gamma, G; J)$$

for the set of all isomorphism classes of J-reduced (Γ, G)-bisets. For $x, y \in W(\Gamma, G; J)$ we define

$$x + y = (x \oplus y)_r,$$
$$x \cdot y = (x *_G y)_r.$$

THEOREM 1.11. *With these operations, $W(\Gamma, G; J)$ is a commutative ring.*

Proof. Everything except the inverse under addition is a routine verification (using 1.10). Let $x \in W(\Gamma, G; J)$. Since $\dot{\bigcup}_{f\in J} x_f$ is J-hyperbolic, the reduced part of $y = \dot{\bigcup}_{f\in J\setminus\{1\}} x_f$ is the inverse of x under addition.

Now we return to (R, G)-algebras. The contravariant equivalence $\mathrm{Alg}_{(R,\Gamma)} \cong \mathrm{Set}_{(\Gamma,G)}$ preserves the $*$-product and the direct sum $\oplus$. Therefore Theorem 1.1 follows from 1.6, and 1.2 follows from 1.7. The subgroup $U_k(R, G)$ of the units of $P(R, G)$ corresponds to a subgroup J_0 of $P(\Gamma, G)$. By [2], $U_k(R, G)$ and therefore also J_0 are finite. By Theorem 1.8, J_0 has the form $\{G_f \mid f \in J\}$, J a finite subgroup of $\mathrm{Hom}_c(\Gamma, G)$. Then K-hyperbolic (R, G)-algebras go to J-hyperbolic (Γ, G)-sets and vice versa. Now Theorems 1.4 and 1.5 follow from the corresponding Theorems 1.10 and 1.11, respectively. Note in particular that $W(R, G; K)$ and $W(\Gamma, G; J)$ are isomorphic rings.

2. Functoriality. Let $\varphi\colon G \to H$ be a homomorphism of finite abelian groups. Recall the definitions of the semirings $P(\Gamma, G)$ and $P(\Gamma, H)$ from the first section. We define

$$P(\varphi)\colon P(\Gamma, G) \to P(\Gamma, H)$$

as follows: $P(\varphi)(X)$ is the (Γ, H)-biset $H *_G X$, where $\alpha(h*x) = h*\alpha x$ and $h'(h*x) = h'h*x$ for $\alpha \in \Gamma$, $h, h' \in H$, $x \in X$. One checks that this is indeed a well-defined (Γ, H)-biset.

THEOREM 2.1. *$P(\varphi)$ is a homomorphism of semirings, i.e. $P(\varphi)$ is compatible with $\oplus$, preserves the neutral element, and*

$$P(\varphi)(X *_G Y) \cong P(\varphi)(X) *_H P(\varphi)(Y)$$

for all $X, Y \in P(\Gamma, G)$.

Proof. Routine calculation.

If J is a finite subgroup of the units of $P(\Gamma, G)$, and $J = P(\varphi)(J)$, then $P(\varphi)(X)$ is J-hyperbolic whenever X is J-hyperbolic. Hence we get a map

$$\begin{aligned} W(\varphi)\colon W(\Gamma, G; J) &\to W(\Gamma, H; J), \\ X &\mapsto (P(\varphi)(X))_r. \end{aligned}$$

THEOREM 2.2. *$W(\varphi)$ is a ring homomorphism.*

Proof. This is essentially a consequence of Theorem 2.1.

THEOREM 2.3. (a) *If φ is injective, then $P(\varphi)$ is injective.*
(b) *If φ is injective, then $W(\varphi)$ is injective.*

Proof. (a) Without loss of generality, φ is an inclusion $G \subset H$. Let X be a (Γ, G)-biset, and let Y be $H *_G X$, considered as a (Γ, G)-biset (not as a (Γ, H)-biset).

Claim. $Y \cong X \dot{\cup} \cdots \dot{\cup} X([H : G]$ copies) as a (Γ, G)-biset.

Proof of the claim. Let $H = \bigcup_{i=1}^{n} h_i G, n = [H : G]$. One checks that $H *_G X = X_1 \dot{\cup} \cdots \dot{\cup} X_n$ as (Γ, G)-bisets where $X_i = \{h_i g * x \mid x \in X, g \in G\}$. Moreover, $X \cong X_i$ by the map $x \mapsto h_i * x$.

Now suppose X and X' are (Γ, G)-bisets such that $P(\varphi)(X) = P(\varphi)(X')$. This implies $Y \cong Y'$ as (Γ, G)-bisets; therefore $X \dot{\cup} \cdots \dot{\cup} X$ (n times)$\cong X' \dot{\cup} \cdots \dot{\cup} X'$ (n times). To infer $X \cong X'$ from this, use the uniqueness of the decomposition into indecomposable bisets.

(b) Let $x \in W(\Gamma, G; J)$, $x \neq 0$. By definition, x is J-reduced. Suppose $W(\varphi)(x) = 0$. This means $P(\varphi)(x) = H *_G x$ is J-hyperbolic. This implies $P(\varphi)(x) *_H P(\varphi)(u) \cong P(\varphi)(x)$ for all $u \in J$. By part (a) and Theorem 2.1, this implies $x *_G u \cong x$ for all $u \in J$, i.e. x is J-hyperbolic, a contradiction.

We consider the group $\mathbf{Q}/\mathbf{Z}$. Let I be the set of all finite subgroups of $\mathbf{Q}/\mathbf{Z}$. Let J be a finite subgroup of the character group $\mathrm{Hom}_c(\Gamma, \mathbf{Q}/\mathbf{Z})$. Then there is a $G \in I$ such that J actually lies in $\mathrm{Hom}_c(\Gamma, G)$. For $H_1, H_2 \in I$, $G \subset H_1 \subset H_2$, let i_{G,H_j} be the inclusion $G \subset H_j$, and i_{H_1,H_2} the inclusion $H_1 \subset H_2$. Denote $P(i_{G,H})(J)$ by J_H. By 2.3, the map

$$W_{H_1,H_2} = W(i_{H_1,H_2}) : W(\Gamma, H_1; J_{H_1}) \to W(\Gamma, H_2; J_{H_2})$$

is injective. We can take the direct limit over the system (W_{H_1,H_2}) and define

$$W(\Gamma, \mathbf{Q}/\mathbf{Z}; J) = \lim_{\substack{\longrightarrow \\ H \supset G}} W(\Gamma, H; J_H).$$

The concepts of the rest of this section are motivated by the phenomenon of ramification in number fields (with some twist of terminology at the infinite primes).

Let Γ, Δ be profinite groups. Given $\varphi_1, \varphi_2 \in \mathrm{Hom}_c(\Gamma, \Delta)$, we define $\varphi_1 \sim \varphi_2$ if there exists $\delta \in \Delta$ such that $\varphi_2(\gamma) = \delta^{-1}\varphi_1(\gamma)\delta$ for all $\gamma \in \Gamma$. A *morphism* for Γ to Δ is an equivalence class $[\varphi]$ with respect to $\sim$. Let G be a finite abelian group and X a (Δ, G)-biset, and $[\varphi]$ a morphism from Γ to Δ. We define a (Γ, G)-biset X_φ by

$$X = X_\varphi \text{ as a set;}$$

$$\mu(\gamma, x) = \varphi(\gamma)x, \quad \nu(\sigma, x) = \sigma x, \qquad (x \in X, \gamma \in \Gamma, \sigma \in G).$$

The isomorphism class of X_φ depends only on $[\varphi]$, as is easily checked. Therefore we have a semiring homomorphism

$$\lambda = P([\varphi], G) \colon P(\Delta, G) \to P(\Gamma, G).$$

Of course, units map to units under λ, and if X is J-hyperbolic, then $\lambda(x)$ is $\lambda(J)$-hyperbolic, so a ring homomorphism

$$W([\varphi], G; J) \colon W(\Delta, G; J) \to W(\Gamma, G; \lambda(J))$$

is induced. Here J is a finite subgroup of $P(\Delta, G)$, or (which is the same by Theorem 1.8) a finite subgroup of $\mathrm{Hom}_c(\Delta, G)$.

A profinite group Ψ is called *procyclic* if it has a topological generator (i.e. it has a cyclic subgroup whose closure is Ψ).

By a *procyclic segment* of a profinite group Γ we mean a pair (Φ, Λ), where Φ is a closed normal subgroup of Λ, Λ is a closed subgroup of Γ containing Φ, and Λ/Φ is procyclic. Let (Φ, Λ) be a procyclic segment of Γ, and X a finite continuous Γ-set. X is called *Φ-unramified,* if $\gamma x = x$ for all $\gamma \in \Phi$, $x \in X$. If X is Φ-unramified, then X is naturally a Λ/Φ-set (as one easily checks). We may write

$$X = X_1 \cup \cdots \cup X_g.$$

where the X_i are transitive Λ/Φ-sets. We define

$$f_i = |X_i|, \qquad i = 1, \ldots, g.$$

Then $|X| = \sum_{i=1}^g f_i$. We call X *normal* if for all $\alpha, \beta \in \Gamma$ and $x \in X$, $\alpha x = x$ implies $\alpha\beta x = \beta x$.

Theorem 2.4. *Assume X is transitive, normal, and Φ-unramified. Then $f_i = f_j$ for all $i, j \in \{1, \ldots, g\}$.*

Proof. Pick $x_i \in X_i$, $x_j \in X_j$. For $k \in \{i, j\}$, let

$$\Lambda_k = \{\lambda \in \Lambda \mid \lambda x_k = x_k\}.$$

Since X is transitive, there is an $\alpha \in \Gamma$ with $\alpha x_i = x_j$. If $\lambda x_i = x_i$, then $\lambda\alpha x_i = \alpha x_i$ by normality; hence $\lambda x_j = x_j$. This implies $\Lambda_i = \Lambda_j$, so $f_i = [\Lambda : \Lambda_i] = [\Lambda : \Lambda_j] = f_j$, which proves the theorem.

Now let G be a finite abelian group. We write $P_u(\Gamma, G)$ for the set of those $X \in P(\Gamma, G)$ which are Φ-unramified. $P_u(\Gamma, G)$ is a subsemiring of $P(\Gamma, G)$. We write

$$\varphi\colon P_u(\Gamma, G) \to P(\Lambda/\Phi, G)$$

for the natural map.

Let J be a finite subgroup of $\mathrm{Hom}_c(\Gamma, G)$ with $f(\Phi) = 1$ for all $f \in J$. We call J *Φ-unramified* and identify it in an obvious way with a subgroup J of $\mathrm{Hom}_c(\Gamma/\Phi, G)$. We restrict this to Λ/Φ to get $J' \subseteq \mathrm{Hom}_c(\Lambda/\Phi, G)$. We write $W_u(\Gamma, G; J)$ for the set of those $X \in P_u(\Gamma, G)$ which are J-reduced. We define

$$\theta\colon W_u(\Gamma, G; J) \to W(\Lambda/\Phi, G; J')$$

by $x \to \varphi(x)_r$.

THEOREM 2.5. *$W_u(\Gamma, G; J)$ is a subring of $W(\Gamma, G; J)$. Also, θ is a ring homomorphism.*

Proof. This is easy to check.

Although the properties of this last map are not clear at the moment, it suggests to examine the special case Γ procyclic more closely.

3. Calculations. As before, let Γ be a profinite group, G a finite abelian group, J a finite subgroup of $\mathrm{Hom}_c(\Gamma, G)$. A (Γ, G)-biset X is called *free*, if for all $x \in X$ and $\sigma \in G$ we have $\sigma x = x$ only for $\sigma = e$. It is easy to see that disjoint union and $*$-product of free bisets are free. This allows us to make the following definitions:

(size of $X =$)$s(X) = |X/G| (= |X|/|G|)$ for X free.

$P_0(\Gamma, G) =$ semiring of isomorphism classes of G-free (Γ, G)-bisets.

$W_0(\Gamma, G; J) =$ ring of isomorphism classes of J-reduced G-free (Γ, G)-bisets.

(Here we also used the trivial fact that the J-reduced part of a free biset is again free.) Note that $s(X \oplus Y) = s(X) + s(Y)$ and $s(X *_G Y) = s(X) \cdot s(Y)$ for X, Y free.

For technical purposes, we define one more notion: A biset X is called *separated* if it is free, indecomposable, and the following holds:

$$\forall \alpha \in \Gamma, \sigma \in G: \quad \alpha x = \sigma x \Rightarrow \alpha x = x.$$

One checks that the separated bisets X correspond to the triples $(\Delta, e, 1)$ in the correspondence of Theorem 1.9.

THEOREM 3.1. *If X and Y are separated of coprime sizes, then $X *_G Y$ is separated.*

Proof. We know that X and Y correspond to triples $(\Delta_1, e, 1)$ and $(\Delta_2, e, 1)$. Therefore, X and Y are isomorphic to $\Gamma/\Delta_1 \times G$ and $\Gamma/\Delta_2 \times G$ respectively, with the canonical $\Gamma \times G$-structure. One verifies:

$$(\Gamma/\Delta_1 \times G) *_G (\Gamma/\Delta_2 \times G) \cong (\Gamma/\Delta_1 \times \Gamma/\Delta_2) \times G,$$

where Γ operates diagonally on $\Gamma/\Delta_1 \times \Delta_2$. Since the numbers $[\Gamma : \Delta_1] = s(X)$ and $[\Gamma \colon \Delta_2] = s(Y)$ are coprime, the

$$\Gamma\text{-set } \Gamma/\Delta_1 \times \Gamma/\Delta_2$$

is canonically isomorphic to the Γ-set $\Gamma/\Delta_1 \cap \Delta_2$. Therefore $X *_G Y$ corresponds to $(\Delta_1 \cap \Delta_2, e, 1)$ and is separated.

For the rest of this section, assume Γ *abelian.*

THEOREM 3.2. *Every separated biset X is uniquely the $*$-product of bisets X_p (p runs over all primes dividing $s(X)$) which are separated and whose size is a power of p.*

Proof. There is an open subgroup $\Delta \subset \Gamma$ such that $X \cong \Gamma/\Delta \times G$ as a biset. Let X_p be a biset of the form $\Gamma/\Delta_p \times G$, $\Delta_p \subset \Gamma$ open, p running over a finite set of primes. Then X is the $*$-product of the X_p if and only if the Γ-sets Γ/Δ and $\prod \Gamma/\Delta_p$ are isomorphic, where Γ operates diagonally on the latter. If $[\Gamma : \Delta_p]$ is assumed to be a power of p, then (as in the last proof)

$$\prod \Gamma/\Delta_p \cong \Gamma/\bigcap \Delta_p \quad \text{as } \Gamma\text{-sets.}$$

Therefore the existence of a product representation as in the theorem is equivalent to the existence of a representation $\Delta = \bigcap \Delta_p$, $[\Gamma : \Delta_p]$ a power of p. The same goes for the uniqueness. Since Γ is abelian, existence and uniqueness of the representation $\Delta = \bigcap \Delta_p$, $[\Gamma : \Delta_p]$ a power of p, follow. This proves the theorem.

Now let $G = C_p$ be cyclic of order p, and let $\Gamma = \hat{\mathbf{Z}}$ be the "proin-tegral" group. Let J be the finite group $\mathrm{Hom}_c(\Gamma, C_p)$.

THEOREM 3.3. (a) *Every reduced indecomposable* (Γ, G)*-set* X *is free.*

(b) *For every reduced indecomposable* X *there is precisely one* $f \in J$ *such that* $X *_G G_f$ *is separated.*

Proof. (a) Let (Δ, H, t) be the triple associated to X. Suppose $H = G$ $(= C_p)$. Then for all $f \in J$, the triple associated to $X *_G G_f$ is $(\Delta, H, f \cdot t)$, and $f \cdot t = t$ (recall $t \colon \Delta \to G/H$, and G/H is the trivial group here). Therefore X is J-hyperbolic. Thus H has to be the trivial group e, and this implies that X is free.

(b) By part (a), X is associated to $(\Delta, e, t), t$ a homomorphism $\Delta \to G$. Suppose that for all $f \in J$ we have $f(\Delta) = 1$. Then $f \cdot t = t$ for all f, and X would be J-hyperbolic. Thus there exists an $f \in J$ with $f(\Delta) \neq 1$, i.e. $\Delta \not\subset p\hat{\mathbf{Z}}$. Then one checks that there is an $f_0 \in \mathrm{Hom}_c(\Gamma, G)$ with $f_0 \mid \Delta = t$. Then $X *_G X_{f_0^{-1}}$ is associated to the triple $(\Delta, e, 1)$, whence it is separated. The uniqueness statement in (b) is easy to check.

Theorem 3.2 motivates the following definition: Let q be a prime. $W_q(\Gamma, G; J)$ is the set of isomorphism classes of J-reduced bisets X which satisfy: Every indecomposable component Y of X has size $s(Y)$ a power of q.

THEOREM 3.4. $W_q = W_q(\Gamma, G; J)$ *is a subring of* $W(\Gamma, G; J)$.

Proof. $G_1 \in W_q$ since $s(G_1) = 1$. W_q is trivially closed under addition. Let X, $Y \in W_q$. We may suppose they are indecomposable and even separated (use 3.3b) and the fact that $G_f \in W_q$ for all $f \in J$. Thus X and Y are isomorphic to $\Gamma/\Delta_1 \times G$ and $\Gamma/\Delta_2 \times G$ respectively, where Δ_1, Δ_2 are open subgroups of Γ with indices q^{e_1} and q^{e_2}, respectively. Hence $X *_G Y \cong (\Gamma/\Delta_1 \times \Gamma/\Delta_2) \times G$, Γ operating diagonally on $\Gamma/\Delta_1 \times \Gamma/\Delta_2$. One checks that $\Gamma/\Delta_1 \times \Gamma/\Delta_2$ is Γ-isomorphic to the disjoint union of $|\Gamma/\Delta_1\Delta_2|$ copies of $\Gamma/\Delta_1 \cap \Delta_2$. Since the index of $\Delta_1 \cap \Delta_2$ in Γ is again a power of q, this proves $X *_G Y \in W_q$.

THEOREM 3.5. *Recall* Γ *was* $\hat{\mathbf{Z}}$ *and* G *was* C_p. *The ring* $W(\Gamma, G; J)$ *is canonically isomorphic to*

$$\bigotimes_{q \text{ prime} \neq p} W_q(\Gamma, G; J),$$

where the tensor product is taken over the ring

$$S = \mathbf{Z}J \Big/ \left(\sum_{f \in J} f \right) \cong \mathbf{Z}[\zeta_p].$$

(The module structure is given by $f \cdot X = X * G_f$*).*

Proof. First claim. $W = W(\Gamma, G; J)$ is S-free on the separated bisets.

Proof of first claim. By 3.3(b), every indecomposable reduced X has the form $f \cdot Y$, with Y separated and $f \in J$. One verifies that the annihilator of Y in $\mathbf{Z}J$ is precisely $(\sum_{f\in J} f)$. (Note $\bigoplus_{f\in J} f \cdot Y$ is J-hyperbolic.)

Second claim. W_p is S-free on the separated bisets whose size is a power of q.

Proof of second claim. Similar to the first one.

Now we can write down all separated bisets X: $X_n = \Gamma/\Delta \times G$ with $\Delta = n\mathbf{Z}$, $n \in \mathbf{N}$. Note $s(X_n) = n$. On the proof of 3.3(b) we saw that X_n is J-hyperbolic if $p \mid n$, so we only take n prime to p. Therefore W has an S-basis

$$\{X_n \mid n \in \mathbf{N},\ (p, n) = 1\}.$$

W_q has an S-basis

$$\{X_{q^e} \mid e \in \mathbf{N}\}$$

for $y \neq p$. There is a canonical ring homomorphism

$$V\colon \bigotimes_{q\neq p} W_q \to W \qquad (\otimes \text{ over } S).$$

We claim it is an isomorphism. As in the proof of 3.4, one works out the multiplication rule

$$X_m \cdot X_n = \gcd(m, n) \cdot X_{\operatorname{lcm}(m,n)}.$$

Using the given S-bases of W_p and W, it is straightforward to check that V is an isomorphism.

To finish this section, we give an explicit description of the ring $W_q = W_q(\hat{\mathbf{Z}}, C_p; J)$. To this end, we define a subring T_q of the ring $S^{\mathbf{N}}$ of infinite sequences in S (addition and multiplication via components). Recall $S \cong \mathbf{Z}[\zeta_p]$, ζ_p a primitive pth root of unity.

$$T_q = (x_\nu) \in S^{\mathbf{N}} \left\{ \begin{array}{l} x_\nu \equiv x_{\nu-1} \operatorname{mod} q^\nu \text{ for all } \nu \geq 1, \\ (x_\nu) \text{ eventually constant.} \end{array} \right.$$

One can define special elements $z_e \in T_q$ $(e \in \mathbf{N})$ as follows:

$$\begin{aligned} z_0 &= (1, 1, 1, 1, \ldots) \\ z_1 &= (0, q, q, q, \ldots) \\ z_2 &= (0, 0, q^2, q^2, \ldots) \\ z_3 &= (0, 0, 0, q^3, \ldots) \\ \vdots \quad & \quad \vdots \end{aligned}$$

Then the z_e form an S-basis of T_q. We can define an isomorphism of S-modules

$$\varphi \colon W_q \to T_q, \qquad \varphi(X_{q^e}) = z_e.$$

The multiplication table for the X_{q^e} is as follows: For $e \leq f$, $X_{q^e} \cdot X_{q^f} = q^e \cdot X_{q^f}$. It is easy to see that for $e \leq f$, we also have $z_e \cdot z_f = q^e \cdot z_f$. Therefore we conclude:

THEOREM 3.6. *$\varphi \colon W_q \to T_q$ is a ring isomorphism.*

We add some remarks about the ring T_q, omitting the (not very difficult) proofs.

1. T_q is connected.
2. If $\overline{q} \subset S$ is a prime over q, then T_q has exactly one prime ideal $Q = (\overline{q}, e_1, e_2, e_3, \cdots)$ over q, and this is maximal.
3. If $\overline{p} \subset S$ is a prime not over q (including the case $\overline{p} = 0$), then there is an infinity of primes $\mathfrak{P}_0, \mathfrak{P}_1, \mathfrak{P}_2, \ldots, \mathfrak{P}_\infty$ over $\overline{p}$. They are defined as follows:

$$\mathfrak{P}_1 = \pi_1^{-1}(\overline{p}) \qquad (\pi_i \colon T_q \to S \text{ is the } i\text{th projection}),$$
$$\mathfrak{P}_\infty = \{(x_\gamma) \in T_q \mid \lim(x_\gamma) \in p\}.$$

(The lim makes sense since (x_γ) is eventually constant.) These are minimal primes with residue class ring $\cong S$ if $\overline{p} = 0$, maximal primes with residue class ring $\cong S/\overline{p}$ otherwise.

Since the absolute Galois group Γ of a finite field k is isomorphic to $\hat{\mathbf{Z}}$, this calculation also applies to the ring $W(k, C_p; K)$, where K is the unique field extension of degree p over k.

References

[1] F. DeMeyer and D. K. Harrison, *Seminar Notes Colorado State University* 1985, to appear.

[2] D. K. Harrison, *Abelian extensions of commutative rings*, in: *Galois Theory and Cohomology of Commutative Rings*, Mem. Amer. Math. Soc., no. 52, 1965.

[3] G. Janusz, *Separable algebras over commutative rings*, Trans. Amer. Math. Soc., **122** (1966), 461–479.

Received October 28, 1987 and in revised form May 3, 1988.

University of München
8000 München 2, F.R. Germany

and

University of Oregon
Eugene, OR 97403