Canad. Math. Bull. Vol. **29** (1), 1986

FUNCTORS ON FINITE VECTOR SPACES AND UNITS IN ABELIAN GROUP RINGS

BY
KLAUS HOECHSMANN

ABSTRACT. If A is an elementary abelian group, let $\dot{U}(A)$ denote the group of units, modulo torsion, of the group ring $\mathbf{Z}[A]$. We study $\dot{U}(A)$ by means of the composite

$$\prod_C \dot{U}(C) \to \dot{U}(A) \to \prod_B \dot{U}(B),$$

where C and B run over all cyclic subgroups and factor-groups, respectively. This map, γ, is known to be injective; its index, too, is known. In this paper, we determine the rank of γ tensored (over $\mathbf{Z}$) with various fields. Our main result depends only on the functoriality of $\dot{U}$.

1. **Introduction**. Let F be a field of $q = p^s$ elements and K be a field whose characteristic does not divide $q - 1$. Letting $\mathcal{V}$ denote the category of finite dimensional vector spaces, consider an arbitrary functor $E : \mathcal{V}(F) \to \mathcal{V}(K)$ such that $E(0) = 0$. We shall be interested in the rank of a certain $\mathcal{V}(K)$-morphism γ obtained, via E, as follows.

Let V be an $(n + 1)$-dimensional F-space, $a_l : F \to V$ and $b_h : V \to F$ be families of rank one maps such that the images of the a_l and the kernels of the b_h are precisely all subspaces of dimension one and codimension one, respectively, each occurring exactly once. Then γ is the composition

$$\prod_l E(F) \xrightarrow{\alpha} E(V) \xrightarrow{\beta} \prod_h E(F),$$

where $\alpha = \prod_l E(a_l)$ and $\beta = \prod_h E(b_h)$.

It turns out that, for $char(K) \neq p$, γ is an isomorphism. In the more interesting case, $char(K) = p$, the rank of γ can be computed by the formula given in the theorem of Part 3 below.

In Part 4 we apply this result to the context which had originally motivated the study of γ: F is the prime field and $E(V)$ comes from the non-torsion units of the integral group ring belonging to the additive group V^+.

2. **Preliminaries**. We need to recall a couple of elementary facts about polynomials. For later reference they will be presented in the form of two lemmas.

Received by the editors August 31, 1984.
AMS Subject Classification: 16A26, 20K05, 13F99, 18F99.

https://doi.org/10.4153/CMB-1986-015-1 Published online by Cambridge University Press

LEMMA 1. *Let $f(X_1, \ldots, X_n)$ be a polynomial of degree d over K. If K has more than d elements, there exist $c_1, \ldots, c_n \in K$ such that $f(c_1, \ldots, c_n) \neq 0$.*

PROOF. Induction on n, the case $n = 1$ being obvious. Writing $f(X_1, \ldots, X_n) = \sum g_k(X_2, \ldots, X_n)X_1^k$, we first find $c_2, \ldots, c_n$ such that $g_m(c_2, \ldots, c_n) \neq 0$ for the highest occurring power X_1^m and then apply the case $n = 1$.

The next lemma is about homogeneous polynomials of degree d, also called d − *forms*, in $n + 1$ indeterminates over K. The set $H(n, d, K)$ of these is a vector space spanned by the monomials $X^{\mathbf{i}} = X_0^{i_0} \cdots X_n^{i_n}$, where $\mathbf{i}$ runs over all $(n + 1)$-tuples of non-negative integers such that $i_0 + \cdots + i_n = d$.

An important subspace $H'(n, d, K)$ consists of those d-forms which involve only the monomials $X^{\mathbf{j}}$ such that

$$\binom{d}{\mathbf{j}} = \frac{d!}{j_0! \cdots j_n!}$$

is non-zero. Note that all d^{th} powers of 1-forms are automatically in $H'(n, d, K)$. It is easy to see that the dimension $h(n, d)$ of $H(n, d, K)$ satisfies $h(n, d) = h(n - 1, d) + h(n, d - 1)$, whence by induction one has the well-known formula

$$h(n, d) = \binom{n + d}{d}.$$

The dimension $h_K(n, d)$ of $H'(n, d, K)$ can be smaller; however, this happens only if $0 < char(K) < d$.

LEMMA 2. *If K has more than d elements, $H'(n, d, K)$ is spanned by the d^{th} powers of 1-forms.*

PROOF. With every $c = (c_1, \ldots, c_n) \in K^n$ we associate the linear form

$$g_c(X) = X_0 + c_1X_1 + \cdots + c_nX_n.$$

With every multi-index $\mathbf{j}$ such that $\binom{d}{\mathbf{j}} \neq 0$ we associate the monomial

$$X^{[\mathbf{j}]} = \binom{d}{\mathbf{j}} X_0^{j_0} \cdots X_n^{j_n}.$$

These monomials form a basis of $H'(n, d, K)$. We shall prove that this space is spanned by the d-forms

$$g_c(X)^d = \sum_{\mathbf{j}} c_1^{j_1} \cdots c_n^{j_n} X^{[\mathbf{j}]}.$$

By Lemma 1, it is impossible to find a non-trivial set of coefficients $a_{\mathbf{j}} \in K$ such that

$$\sum_{\mathbf{j}} a_{\mathbf{j}} c_1^{j_1} \cdots c_n^{j_n} = 0$$

for all $c \in K^n$. This means that the matrix $c_1^{j_1} \cdots c_n^{j_n}$, whose $h_K(n, d)$ columns are

https://doi.org/10.4153/CMB-1986-015-1 Published online by Cambridge University Press

labelled by $\mathbf{j}$ and whose (perhaps infinitely many) rows are labelled by c, has rank $h_K(n,d)$. Hence there are that many linearly independent forms $g_c(X)^d$.

DEFINITION. *A subset of non-trivial elements of a vector space V will be called* projective *if it contains exactly one element of every 1-dimensional subspace of V.*

PROPOSITION 1. *Let F be a field of q elements, ϕ a non-degenerate bilinear form on F^{n+1}, and $P \subset F^{n+1}$ a projective subset. For $0 < d < q$, consider the matrix*

$$M(x,y) = \phi(x,y)^d$$

defined on $P \times P$. Then M has rank $h_F(n,d)$.

PROOF. If we replace an element $x \in P$ by a non-trivial multiple cx, the corresponding row of M is multiplied by c^d. If we replace ϕ by ψ where $\psi(x,y) = \phi(Tx,y)$ for some invertible linear T, the rows are permuted and modified as above. Neither of these operations affects the rank. Without loss of generality, we may therefore take

$$\phi(x,y) = \sum_{k=0}^{n} x_k y_k.$$

If we enlarge the matrix by allowing x to run over all of F^{n+1}, we are only adjoining multiples of rows that are already there. Ditto for columns. We may therefore work with the larger matrix M^o defined on the index set $F^{n+1} \times F^{n+1}$ by

$$M^o(x,y) = \left(\sum_{k=0}^{n} x_k y_k\right)^d.$$

Each row of this matrix consists of all possible evaluations of the d-form

$$\left(\sum_{k=0}^{n} x_k X_k\right)^d.$$

As x runs over F^{n+1}, there are exactly $h_K(n,d)$ linearly independent such forms, by Lemma 2. The q^{n+1}-tuples of their evaluations remain independent by Lemma 1.

3. **The result**. Returning now to the context of the introduction, note that every object V of $\mathcal{V}(F)$ is automatically a G-module, where $G = Aut(F^+) = F^\times$, and so is its image $E(V)$. Since the order of G is prime to $char(K)$, the G-modules $E(F), E(V)$, etc. are semi-simple.

As the rank of γ is not affected by extension of K, we may take K to be algebraically closed. Then $E(F)$ is a direct sum, over some index set I, of 1-dimensional G-modules W_i, $(i \in I)$, on each of which G acts via a character $\mu_i : G \to K^\times$. In case $char(K) = p$, F can be identified with a subfield of K, and these characters are simply the d^{th} powers of the inclusion, with $d = 1, \ldots, q-1$. We let m_d denote the multiplicity of the d^{th}-power character in the G-module $E(F)$.

THEOREM. *Let V, E, γ be as in the introduction.*
(a) *If $char(K) \neq p$, γ is an isomorphism.*

https://doi.org/10.4153/CMB-1986-015-1 Published online by Cambridge University Press

(b) *If* $char(K) = p$, *the rank of* γ *is*

$$\sum_{d=1}^{q-1} m_d h_K(n,d).$$

PROOF. It is convenient to use some non-degenerate bilinear form ϕ on V in order to identify hyperplanes with lines and to parametrize the latter by some projective subset $P \subset V$. γ thus appears as an endomorphism of the K-space

$$L = \prod_{x \in P} E(F)$$

given by the $P \times P$-matrix $\beta_y \circ \alpha_x$, with $\alpha_x : E(F) \to E(V)$, $\beta_y : E(V) \to E(F)$ being the functorial images of $a_x : F \to V$, $b_y : V \to F$, respectively. Since $b_y \circ a_x = \phi(x,y)$ is either trivial or in G the same goes for $\beta_y \circ \alpha_x$.

Now, G acts diagonally on the product L, and γ is a G-morphism. Therefore γ is a direct sum of endomorphisms $\gamma_i : L_i \to L_i$, where $L_i = \prod_{x \in P} W_i$ is made up of $|P|$ copies of the 1-dimensional K-space W_i, on which G acts via μ_i, as described at the beginning of this paragraph. γ_i is given by the $P \times P$-matrix

$$M_i = \mu_i(\phi(x,y))$$

with entries in K.

It remains to be shown that, for any multiplicative character μ on F, the $P \times P$-matrix $M(x,y) = \mu(\phi(x,y))$ is non-singular, in case (a), and has rank $h_K(n,d)$, in case (b). The latter being immediate from Proposition 1, we are reduced to case (a).

Let $M^*(x,y) = \mu^{-1}(\phi(x,y))$ and consider the product $S = MM^*$. It is shown in [2] that $S(x,x) = q^n$ and that, for $x \neq y$,

$$(q-1)S(x,y) = q^{n-1} \sum_a \mu(a) \sum_b \mu^{-1}(b)$$

with $a, b \in F$. If $\mu \neq 1$, the latter yields 0. For $\mu = 1$, we get $S(x,y) = q^{n-1}(q-1)$. Since $q \neq 0$ in K, we can say that $q^{-n+1}S$ has q on, and $q-1$ off, the diagonal. Adding all rows into the first one, we obtain there $q|P| - |P| + 1 = q^{n+1}$, in each column. Hence $q^{-n+1}S$ has determinant q^{n+1}.

4. **An application**. We shall apply the theorem to study the group of units modulo torsion, $\dot{U}(V^+)$, of the group ring $\mathbf{Z}[V^+]$, taking F to be the prime field. When we need to consider the group of units, again modulo torsion, of an algebraic number field $\mathbf{Q}(\theta)$, we shall use the abbreviation $\dot{U}(\theta)$.

Let ϵ be a p^{th} root of unity. The Wedderburn isomorphism $\mathbf{Q}[F^+] \to \mathbf{Q} \oplus \mathbf{Q}[\epsilon]$ yields an injection $\mathbf{Z}[F^+] \to \mathbf{Z} \oplus \mathbf{Z}[\epsilon]$, whence an injection $\dot{U}(F^+) \to \dot{U}(\epsilon)$ of finite index (cf. [3], II.2.9, p. 49). By Dirichlet's Unit Theorem, $\dot{U}(\epsilon)$ and $\dot{U}(\epsilon + \epsilon^{-1})$ have the same rank $(p-3)/2$, and hence we have an isomorphism

$$\dot{U}(F^+) \otimes \mathbf{Q} \to \dot{U}(\epsilon + \epsilon^{-1}) \otimes \mathbf{Q}$$

with the unit group in additive notation and $\otimes$ meaning tensor over $\mathbf{Z}$. Now

Minkowski's Unit Theorem (cf. [1], Anhang, p. 271) implies that the latter is G_0-isomorphic to $\mathbf{Q}[G_0]$ modulo "traces", where $G_0 = G/\{\pm 1\}$ is the Galois group of $\mathbf{Q}[\epsilon + \epsilon^{-1}]$. The upshot of all this is that the G-module $\dot{U}(F^+)$ involves only the non-trivial *even* characters of G, each of them with multiplicity 1.

Again working with duality and a projective subset $P \subset V$, we obtain an endomorphism $\dot{\gamma}$ of the lattice $\Lambda = \prod_{x \in P} \dot{U}(F^+)$ as a composition

$$\Lambda \xrightarrow{\dot{\alpha}} \dot{U}(V^+) \xrightarrow{\dot{\beta}} \Lambda,$$

exactly as before, except for the minor fact that here we are dealing with $\mathbf{Z}$-modules instead of vector spaces. We are ultimately interested in the module $\dot{U}(V^+)/\dot{\alpha}(\Lambda)$, which measures the extent to which the units of $\mathbf{Z}[V^+]$ do not come from cyclic subgroups. Now, $\dot{\beta}$ induces an injection of this module into the cokernal $\Gamma = \Lambda/\dot{\gamma}(\Lambda)$ of $\dot{\gamma}$, and we are led to study Γ as a first approximation of our goal.

In [2] the order of Γ was shown to be $p^{(n/2)R}$, where $R = ((p-3)/2)|P|$ is the rank of Λ. Our present purpose is to determine the p-rank of Γ, i.e. the number of its cyclic summands or, equivalently, the dimension of the F-space $\Gamma \otimes F = \Gamma/p\Gamma$. Tensoring the exact sequence

$$\Lambda \xrightarrow{\dot{\gamma}} \Lambda \to \Gamma \to 0$$

with F, we see that $dim\Gamma/p\Gamma$ equals the corank of $\gamma = \dot{\gamma} \otimes F$, which can be read off from the theorem by taking for E the functor $\dot{U}(-) \otimes F$. We obtain

PROPOSITION 2. $dim\Gamma/p\Gamma = R - \Sigma_d h(n,d)$, *where d runs over all even numbers between* 1 *and* $p-2$.

COROLLARY. Γ is elementary abelian if and only if $n \leq 1$.

PROOF. Γ is elementary abelian if and only if $(n/2)R = R - \Sigma_d h(n,d)$ or $(1-(n/2))R = \Sigma_d h(n,d)$. Since the right hand side of the latter expressions is positive, the cases $n \geq 2$ are ruled out. For $n = 1$, we have to verify that $(1/2)R = \Sigma_d h(1,d)$. Now, $h(1,d) = d + 1$, and the right side is $((p-3)/4)\,(p+1)$, which is exactly $(1/2)R$. For $n = 0$, Γ is, of course, trivial.

REFERENCES

1. H. Hasse, *Vorlesungen über Klassenkörpertheorie*, Physica-Verlag, Würzburg (1967).

2. K. Hoechsmann, S. K. Sehgal, A. Weiss, *Cyclotomic Units and the Unit Group of an Elementary Abelian Group Ring*, to appear.

3. S. K. Sehgal, *Topics in Group Rings*, Marcel Dekker, New York (1978).

DEPARTMENT OF MATHEMATICS
UNIVERSITY OF BRITISH COLUMBIA
VANCOUVER, B.C.