K_0 of Hall's Universal Group

Stephen Donkin
Department of Mathematics
University of York
Heslington
York YO10 5DD , England UK

25th August 2005

0. Introduction

Let U denote Hall's universal group. Thus U is countable, locally finite, contains a copy of every finite group and isomorphic finite subgroups of U are conjugate in U. Moreover, U is characterized by these properties (see [2]). From the local finiteness of U it follows that $K_0(\mathbb{C}U)$ is the direct limit of the Grothendieck groups of the its finite subgroups. Thus $K_0(\mathbb{C}U)$ is made up from the character theory of all finite groups and we found it of interest to see how all these character theories fit together. We write $X(U)$ for $K_0(\mathbb{C}U)$. There is a natural ring structure on $X(U)$ and a natural ring homomorphism $\epsilon : X(U) \to \mathbb{Z}$. Since $X(U)$ is a limit of torsion free groups, it is torsion free. The rational Grothendieck group $\mathbb{Q} \otimes_{\mathbb{Z}} X(U)$ has a very simple structure. There is, for each positive integer n, an element c_n of $X(U)$, defined by an element of U of order n. The elements c_n form a $\mathbb{Q}$-basis of $\mathbb{Q} \otimes_{\mathbb{Z}} X(U)$ and multiply according to the rule $c_m c_n = c_r$, where r is the least common multiple of m and n.

The structure of $X(U)$ itself is only slightly more complicated. For each prime p, we write $X_p(U)$ for the subgroup of $X(U)$ generated by the image of Grothendieck groups of finite p-groups. Each $X_p(U)$ is a subring of $X(U)$ and we have $X(U) = \otimes_p X_p(U)$, the tensor product is taken over $\mathbb{Z}$ and p runs over all primes. To further elucidate the structure of $X(U)$ we consider the kernel $I_p(U)$ of the restriction $\epsilon_p : X_p(U) \to \mathbb{Z}$ of $\epsilon : X(U) \to \mathbb{Z}$. We show that $I_p(U)$ is p-divisible and, as a $\mathbb{Z}[1/p]$-module, is free on basis $1-c_p, 1-c_{p^2}, 1-c_{p^3}, \ldots$. Thus we have $X_p(U) = \mathbb{Z} \oplus (\oplus_{r\geq 1} \mathbb{Z}[1/p](1-c_{p^r}))$. Putting all this together, we obtain the concrete description $X(U) = \oplus_{n=1}^{\infty} \mathbb{Z}[1/n]\tilde{c}_n$, where $\tilde{c}_1 = c_1 = 1$ and

$\tilde{c}_n = (c_{q_1}-1)(c_{q_2}-1)\dots(c_{q_r}-1)$, for $n = q_1q_2\dots q_r$, with $q_1,\dots,q_r > 1$ powers of distinct primes.

This paper was written while the author enjoyed the hospitality and support of the Centre Interfacultaire Bernoulli during programme in Group Representation Theory, January to July 2005.

1. Rational Structure

Let G be a locally finite group.We write $\mathrm{proj}(G)$ for the category of finitely generated projective $\mathbb{C}G$-modules and module homomorphisms. If $\phi : G \to H$ is an isomorphism of locally finite groups and $V \in \mathrm{proj}\,\mathbb{C}H$ then we write V^ϕ for the vector space V regarded as an element of $\mathrm{proj}\,\mathbb{C}G$ via the action $g \cdot v = \phi(g)v$, $g \in G$, $v \in V$.

We write $X(G)$ for the Grothendieck group $K_0(\mathbb{C}G) = K_0(\mathrm{proj}\,\mathbb{C}G)$. Let H be a subgroup of G. We have the induction functor from $\mathrm{proj}\,\mathbb{C}H$ to $\mathrm{proj}\,\mathbb{C}G$ taking $V \in \mathrm{proj}\,\mathbb{C}H$ to the induced module $V\uparrow_H^G = \mathbb{C}G \otimes_{\mathbb{C}H} V$. We write ind_H^G for the group homomorphism from $X(H)$ to $X(G)$ given by induction. Let $\mathcal{F}(G)$ denote the directed system of all finite subgroups of G. With respect to the homomorphisms $\mathrm{ind}_H^K : X(H) \to X(K)$, for $H, K \in \mathcal{F}(G)$, with $H \le K$, we have $X(G) = \varinjlim X(H)$. We obtain, in particular, that $X(G)$ is torsion free since each $X(H)$ (H finite) is. We write $X(G)_\mathbb{Q}$ for $\mathbb{Q} \otimes_\mathbb{Z} X(G)$ and identify $X(G)$ with a subgroup of $\mathbb{Q} \otimes_\mathbb{Z} X(G)$.

In case G is finite, we have the natural isomorphism $\mathrm{ch} : X(G) \to \mathrm{char}(G)$, where $\mathrm{char}(G)$ denotes the group of generalized characters of G. Thus, for $V, W \in \mathrm{proj}\,\mathbb{C}G$ and $\phi = [V] - [W] \in X(G)$, we have $\mathrm{ch}(\phi)(x) = \mathrm{trace}(x, V) - \mathrm{trace}(x, W)$, for $x \in G$.

In general we have the " "augmentation homormorphism" $\epsilon_G : X(G) \to \mathbb{Z}$, given by $\epsilon_G([V]) = \dim H_0(G, V)$, for $V \in \mathrm{proj}\,\mathbb{C}G$. Note that, by Frobenius Reciprocity, we have $\epsilon_G \circ \mathrm{ind}_H^G = \epsilon_H$, for a subgroup H of G.

By abuse of notation, we also write ind_H^G and ϵ_G for the $\mathbb{Q}$ linear maps $X(H)_\mathbb{Q} \to X(G)_\mathbb{Q}$ and $X(G)_\mathbb{Q} \to \mathbb{Q}$, obtained from $\mathrm{ind}_H^G : X(H) \to X(G)$ and $\epsilon_G : X(G) \to \mathbb{Z}$ by base change.

We write $\mathrm{Aut}(G)$ for the automorphism group of G, and for a subgroup H of G, write $N_G(H)$ for the normalizer of H in G. Recall that, for $H \in \mathcal{F}(U)$, the natural map $N_U(H) \to \mathrm{Aut}(H)$ is surjective. [There is a subgroup Y, say, of U isomorphic to the holomorph of H. Then Y has a normal subgroup A isomorphic to H and the natural map

$Y \to \mathrm{Aut}(A)$ surjective. Thus $N_U(A) \to \mathrm{Aut}(A)$ is onto. But H is isomorphic to A and hence conjugate in U to A so that $N_U(H) \to \mathrm{Aut}(H)$ is also surjective.] It follows that if $\phi : H \to K$ is an isomorphism between finite subgroups H, K of U then there exists an element $g \in G$ such that $\phi(x) = gxg^{-1}$ for all $x \in H$. Now if $V \in \mathrm{proj}\, \mathbb{C}K$ then we have an isomorphism $\Phi : V^{\phi} \uparrow_H^U \to V \uparrow_K^U$ satisfying $\Phi(1 \otimes v) = g^{-1} \otimes v$, for $v \in V$. Thus we have the following.

(1) *Suppose $H, K \in \mathcal{F}(U)$ and $\phi : H \to K$ is an isomorphism. Then, for $V \in \mathrm{proj}\, \mathbb{C}K$ we have $\mathrm{ind}_H^U([V^{\phi}]) = \mathrm{ind}_K^U([V])$ and in particular $\mathrm{ind}_H^U([V^{\phi}]) = \mathrm{ind}_H^U([V])$ for $\phi \in \mathrm{Aut}(H)$.*

Now G be any finite group and let V be a finite dimensional $\mathbb{C}G$-module. Then we may choose $H \in \mathcal{F}(U)$ and an isomorphism $\phi : H \to G$. Then it follows from (1) that the the element $[V^{\phi} \uparrow_H^U]$ of $X(U)$ is independent of the choice of H and ϕ. We denote this element by $e_{G,V}$. We write simply e_G for $e_{G,V}$ with V the (one dimensional) trivial module. Since $X(U)$ is the direct limit of the $X(H)$ with $H \in \mathcal{F}(U)$ we get that $X(U)$ is generated by all elements $e_{G,V}$ but in fact we have:

(2) *$X(U)$ is spanned by all elements e_G, G finite.*

Proof. Let $\phi \in X(U)$. Then we have $\phi = \mathrm{ind}_H^U(\psi)$, for some $H \in \mathcal{F}(U)$ and $\psi \in X(H)$. Let J be a subgroup of U containing H such that J is isomorphic to a symmetric group. Then $\phi = \mathrm{ind}_J^U(\mathrm{ind}_H^J(\psi))$ so that we may replace H by J and ψ by $\mathrm{ind}_H^J(\psi)$, that is, we may assume that H is a symmetric group. Now it is well know that the group of generalized characters of a symmetric group is generated by permutation characters. Thus we have $\psi = \sum_{i=1}^r a_i \mathrm{ind}_{H_i}^H([\mathbb{C}])$, some some integers $a_1, \ldots, a_r$ and subgroups $H_1, H_2, \ldots, H_r$. Hence we have $\phi = \sum_{i=1}^r a_i \mathrm{ind}_{H_i}^U(\mathbb{C}) = \sum_{i=1}^r a_i e_{H_i}$.

We now construct some elements of $X(U)$ which we will show form a $\mathbb{Q}$-basis of $X(U)_{\mathbb{Q}}$. Let $g \in U$ and let n be the order of n. We write c'_g for the element of $X(\langle g \rangle)_{\mathbb{Q}}$ such that the character of c'_g takes the value n on g and 0 on all other elements. We write c_g for $\mathrm{ind}_{\langle g \rangle}^U(c'_g) \in X(U)_{\mathbb{Q}}$. Let H be a subgroup of U containing g which is isomorphic to the symmetric group $\mathrm{Sym}(n)$ of degree n. Let $b = \mathrm{ind}_{\langle g \rangle}^U(c'_g) \in X(H)_{\mathbb{Q}}$ and let ϕ denote the character of b. Then ϕ takes the value 1 on all elements of H of order n and 0 on all other elements. For an irreducible character χ of H we have $(\phi, \chi) = \chi(g)$. As is well known, all character values of $\mathrm{Sym}(n)$ are integers. Hence $(\phi, \chi) \in \mathbb{Z}$, for all characters of

H so that ϕ is a generalized character and $b \in X(H)$. By transitivity of induction we have $c_g = \mathrm{ind}_H^U(b) \in X(U)$. Moreover, if g' is another element of U of order n, then g' is contained in a subgroup H' of U isomorphic to $\mathrm{Sym}(n)$ and the element $c_{g'}$ of $X(U)$ is induced from the element b' of $X(H')$ whose character is 1 on all elements of H' of order n and 0 on all other elements. Since the groups H and H' are conjugate in U we have $\mathrm{ind}_H^U(b) = \mathrm{ind}_{H'}^{U'}$ and hence $c_g = c_{g'}$. Hence the element c_g depends only on n and we write simply c_n for c_g.

Let $G \in \mathcal{F}(U)$, let $V \in \mathrm{proj}\,\mathbb{C}G$ have character χ. We shall work in $X(U)_{\mathbb{C}} = \mathbb{C} \otimes_{\mathbb{Z}} X(U)$ and identify $X(U)_{\mathbb{Q}}$ with a subgroup of $X(U)_{\mathbb{C}}$. For a positive integer r we write $G(r)$ for the set of all elements of order r. Suppose G contains an element of order r, let $C_{r1}, \ldots, C_{rd_r}$ be the conjugacy classes of G contained in $G(r)$ and let g_{rj} be an element of C_{rj}, for $1 \leq j \leq d_r$. Let G_{rj} be the subgroup generated by g_{rj} and let ϕ_{rj} be the character of $\mathrm{ind}_{G_{rj}}^G(c'_{g_{rj}})$, for $1 \leq j \leq d_r$. Then the value of ϕ_{rj} is the order of the centralizer $Z_G(g_{rj})$ on the class C_{rj} and is 0 elsewhere. Hence we get $\chi = \sum_{r,j} \chi(g_{rj}) \frac{\phi_{rj}}{|Z_G(g_{rj})|}$. Thus $|G|\chi$ is the character of $\sum_{g \in G} \chi(g) \mathrm{ind}_{\langle g \rangle}^G(c'_g)$ so we have $[V] = \frac{1}{|G|} \sum_{g \in G} \chi(g) \mathrm{ind}_{\langle g \rangle}^G(c'_g)$ in $X(G)_{\mathbb{C}}$. Thus we have the following:

(3) *Let G be a finite group and V a finite dimensional $\mathbb{C}G$-module with character χ. Then we have the formula $e_{G,V} = \frac{1}{|G|} \sum_{g \in G} \chi(g) c_g$ in $X(U)_{\mathbb{C}}$. In particular we have $e_G = \frac{1}{|G|} \sum_{r=1}^{\infty} |G(r)| c_r$, in $X(U)_{\mathbb{Q}}$.*

(4) *The elements $c_1, c_2, \ldots$ form a $\mathbb{Q}$-basis of $X(U)_{\mathbb{Q}}$.*

Proof. From (2) and (3) the elements $c_1, c_2, \ldots$ form a spanning set.

Now suppose we have $\sum_{i=1}^n a_i c_i = 0$, with all a_i rational, not all zero. Thus we have $\sum_{i=1}^n a_i \mathrm{ind}_{G_i}^U(c'_{g_i}) = 0$, where g_i is an element of order i and where G_i is the subgroup generated by g_i, for $1 \leq i \leq n$. Let G be a finite subgroup of U containing $g_1, g_2, \ldots$. Then we have $\mathrm{ind}_G^U(\sum_{i=1}^n a_i \mathrm{ind}_{G_i}^G(c'_{g_i})) = 0$. Hence there is a finite subgroup H of U containing G such that $\mathrm{ind}_G^H(\sum_{i=1}^n a_i \mathrm{ind}_{G_i}^G(c'_{g_i}) = 0$. Replacing G by H we may suppose that $\sum_{i=1}^n a_i \mathrm{ind}_{G_i}^G(c'_{g_i}) = 0$. However, the character of $\sum_{i=1}^n a_i \mathrm{ind}_{G_i}^G(c'_{g_i})$ takes the value $a_i |Z_G(g_i)|$ on g_i, which gives $a_i = 0$, for $1 \leq i \leq n$. Hence the elements $c_1, c_2, \ldots$ are linearly independent and so form a basis.

We now introduce a $\mathbb{Q}$-linear product structure on $X(U)_{\mathbb{Q}}$ by declaring $c_r c_s = c_t$, where t is the least common multiple of r and s. Thus $X(U)_{\mathbb{Q}}$ is a commutative, associative algebra. Indeed, $X(U)_{\mathbb{Q}}$ is the monoid algebra on the monoid $\{c_r|r \geq 1\}$. We extend the $\mathbb{Q}$-algebra structure on $X(U)_{\mathbb{Q}}$ to a $\mathbb{C}$-algebra structure on $X(U)_{\mathbb{C}}$ by base change. For $\mathbb{C}$ vector spaces (or $\mathbb{C}G$-modules, G a finite group) V, W we write simply $V \otimes W$ for the vector space (or $\mathbb{C}G$-module) $V \otimes_{\mathbb{C}} W$.

From (3) we obtain the following.

(5) *Let G and H be finite groups and let V be a finite dimensional $\mathbb{C}G$-module and W be a finite dimensional $\mathbb{C}H$-module. Then, in $X(U)$ we have $e_{G,V}e_{H,W} = e_{G\times H,V\otimes W}$. In particular we have $e_G e_H = e_{G\times H}$.*

Remark One may introduce the product structure on $X(U)$ in a more natural manner in the following way. Since $U \times U$ is a locally finite countable group there is an embedding of $U \times U$ into U. Hence we have a homomorphism $X(U \times U) \to X(U)$, moreover we have the natural isomorphism $X(U) \otimes_{\mathbb{Z}} X(U) \to X(U \times U)$ and hence a group homomorhism $X(U) \otimes_{\mathbb{Z}} X(U) \to X(U)$. We leave it to the reader to check that this product structure is independent of the choice of embedding $U \times U \to U$ and agrees with the one introduced above.

(6) *(i) For G a finite group and V a simple $\mathbb{C}G$-module we have*

$$\epsilon(e_{G,V}) = \begin{cases} 1, & \text{if } V \textit{ is trivial} \\ 0, & \text{otherwise.} \end{cases}$$

In particular we have $\epsilon(e_G) = 1$.
(ii) $\epsilon(c_n) = 1$ for all integers n.
(iii) $\epsilon : X(U) \to \mathbb{Z}$ is a ring homomorphism.

Proof. (i) Let $\phi : H \to G$ be an isomorphism from a subgroup H of U onto V. Then we have $e_{G,V} = \mathrm{ind}_H^U([W])$, where $W = V^{\phi}$. Hence we have $\epsilon(e_{G,V}) = \epsilon(\mathrm{ind}_H^U([W]) = \epsilon_H([W]) = \dim H_0(H, W)$, which is 1 if W (and hence V) if trivial and 0 if W (and hence V) is non-trivial.
(ii) Let $n \geq 1$ and suppose that $\epsilon(c_r) = 1$ for all $1 \leq r < n$. We take G to be a cyclic group of order n. Then we have $ne_G = \sum_{r=1}^n |G(r)|c_r$. Applying ϵ and using the induction hypothesis we get we get $n = |G| - |G(n)| + |G(n)|\epsilon(c_n)$ and hence $\epsilon(c_n) = 1$.
(iii) Clear.

To summarize, we have shown that $X(U)_{\mathbb{Q}}$ is naturally isomorphic, as an augmented algebra, to the monoid algebra $\mathbb{Q}M$, where M is the monoid of positive integers and product $m * n$ being the least common multiple of m and n.

2. Local Structure

We fix a prime p and write $X_p(U)$ for the subgroup of $X(U)$ generated by all elements $e_{G,V}$, where G is a p-group. By §1,(5), $X_p(U)$ is a subring of $X(U)$. Let $\epsilon_p : X_p(U) \to \mathbb{Z}$ be the restriction of $\epsilon : X(U) \to \mathbb{Z}$ and let $I_p(U)$ be the kernel of ϵ_p. For a finite group G and finite dimensional $\mathbb{C}G$-module V affording the representation $\rho : G \to \mathrm{GL}(V)$ we also write $e_{G,\rho}$ for $e_{G,V}$. The main technical point needed to elucidate the structure of $X_p(U)$ that $I_p(U)$ is a p-divisible group. It will be useful to know the following.

(1) *The group $I_p(U)$ is generated by the elements $e_G - e_H$, for all finite p-groups G, H together with all elements $e_{G,\lambda}$, for G a finite group and $\lambda : G \to \mathbb{C}^\times$ a non-trivial homomorphism.*

Proof. Let $\phi \in X_p(U)$ with $\epsilon(\phi) = 0$. Then ϕ has the form $\sum_{i=1}^n a_i e_{G_i,V_i}$, for finite groups $G_1, G_2, \ldots, G_n$ and modules $V_1, V_2, \ldots, V_n$ with $\sum_{i=1}^n a_i \epsilon(e_{G,V_i}) = 0$. Hence $I_p(U)$ is generated by all elements $e_{G,V} - \epsilon(e_{G,V})1$. Furthermore, we may assume that V is irreducible. Hence $I_p(U)$ is generated by all elements $e_G - 1$ and $e_{G,V}$ with V irreducible and non-trivial. For such V we have $e_{G,V} = \mathrm{ind}_H^U([W])$ for a suitable p subgroup of U and non-trivial irreducible $\mathbb{C}H$-module W. However, and irreducible module for a p-groups is induced from a one dimensional module for a subgroup. Hence we have $[W] = \mathrm{ind}_J^H([L])$, for some subgroup J and one dimensional $\mathbb{C}J$-module. Hence we get $e_{G,V} = \mathrm{ind}_H^U([L])$, which gives $e_{G,V} = e_{J,\lambda}$, where $\lambda : J \to \mathbb{C}^\times$ is the representation afforded by L.

We define $X_p(U)^0$ to be the subgroup of $X_p(U)$ generated by all elements e_G, with G a p-group. Thus, by §1,(5), $X_p(U)^0$ is a subring of $X_p(U)$. We write $I_p(U)^0$ for $X_p(U)^0 \cap I_p(U)$.

(2) *Let G be a p-group and $\lambda : G \to \mathbb{C}^\times$ be a homomorphism. Then we have $e_{G,\lambda} = e_{G,\lambda^i}$, for all integers i prime to p.*

Proof. From §1,(3) we have $e_{G,\lambda} = \sum_r (\lambda, \eta_{G(r)}) c_r$, where $\eta_{G(r)}$ is the characteristic function on $G(r)$, and r runs over all powers of p. So the result follows from the fact that $G(r) = \{x^i | x \in G(r)\}$ for all such r.

We consider a finite p subgroup G and a non-trivial homomorphism $\lambda : G \to \mathbb{C}^\times$. Let N be the kernel of λ and let $|G/N| = p^m$. The character $1_G + \lambda + \lambda^2 + \cdots + \lambda^{p^m-1}$ is the character of $\mathbb{C} \uparrow_N^G$. Writing V_i for a $\mathbb{C}G$-module affording λ^i, we get that $\oplus_{i=1}^{p^m} V_i$ is isomorphic to $\mathbb{C} \uparrow_N^G$.

Now G/N is cyclic. Let M be the subgroup of G containing N such that M/N is cyclic of order p. Then we have that $\oplus_{i=1}^{p^{m-1}} V_{pi}$ is isomorphic to $\mathbb{C}\uparrow_N^G$. Hence we have that $(\oplus_{1\leq i\leq p^m,(i,p)=1}V_i)\oplus\mathbb{C}\uparrow_M^G$ is isomorphic to $\mathbb{C}\uparrow_N^G$. Passing to the Grothendieck group of $\mathbb{C}G$-modules, applying ind_G^U and using (3), we get $(p^m-p^{m-1})e_{G,\lambda}=e_N-e_M$.

(3) *(i) For a p-group G and non-trivial homomorphism $\lambda : G\to\mathbb{C}^\times$ with kernel N and G/N of order p^m we have $(p^m-p^{m-1})e_{G,\lambda}=e_N-e_M$, where M is the subgroup of G containing N such that M/N has order p.*
(ii) We have $e_G-e_N\in(p-1)I_p(U)$, for all p-groups G,N, and hence $I_p(U)^0\leq(p-1)I_p(U)$.

Proof. (i) has already been proved. To prove (ii) it suffices to prove that e_G-1 is divisble by $p-1$ in $X(U)$. We suppose G is non-trivial and choose a (normal) subgroup of index p. Let $\lambda : G\to\mathbb{C}^\times$ be a homomorphism with kernel N. We get $e_G-e_N\in(p-1)I_p(U)$ from (i). We may assume, inductively, that $e_N-1\in(p-1)I_p(U)$ and hence $e_G-1=e_G-e_N+e_N-1\in(p-1)I_p(U)$.

(4) *We have $\frac{1}{p^k}(p-1)(1-c_{p^m})\in I_p(U)$ for all integers $k,m\geq 0$.*

Proof. The result is trivially true for $m=0$ and all k. Let $m\geq 1$ and suppose that $\frac{1}{p^k}(p-1)(1-c_{p^i})\in I_p(U)$ whenever $k\geq 0$ and $1\leq i<m$. Let G be a cyclic group of order p^m and let $e=e_G$. Then we have

$$e=\frac{1}{p^m}(1+(p-1)c_p+(p^2-1)c_{p^2}+\cdots+(p^m-p^{m-1})c_{p^m})$$

and hence

$$1-e=\frac{1}{p^m}(p-1)((1-c_p)+p(1-c_{p^2})+\cdots+p^{m-1}(1-c_{p^m}).$$

Hence, by the inductive hypothesis, we get $\frac{1}{p}(1-c_{p^m})\in I_p(U)^0$. Suppose now that $k\geq 1$ and $\frac{1}{p^k}(p-1)(1-c_{p^m})\in I_p(U)^0$. Then we get $\frac{1}{p}(p-1)(1-c_{p^m})\frac{1}{p^k}(p-1)(1-c_{p^m})\in I_p(U)^0$ and hence $\dfrac{(p-1)^2}{p^{k+1}}(1-c_{p^m})\in I_p(U)^0$, i.e. $\dfrac{p(p-1)-(p-1)}{p^{k+1}}(1-c_{p^m})\in I_p(U)^0$. We get $\dfrac{1}{p^{k+1}}(p-1)(1-c_{p^m})\in I_p(U)^0$ and hence $\dfrac{1}{p^k}(p-1)(1-c_{p^m})\in I_p(U)^0$, for all m$k\geq 1$ by induction on k. Hence we also have $\dfrac{1}{p^k}(p-1)(1-c_{p^m})\in$

$I_p(U)$ for all $k \geq 1$, $m \geq 0$ by induction on m. Certainly we must also have $(p-1)(1-c_{p^m}) \in I_p(U)$, for all m.

(5) *We have* $I_p(U)^0 = (p-1)\sum_{r\geq 1} \mathbb{Z}[1/p](1-p^r)$.

Proof. We set $I_p(U)' = (p-1)\sum_{r\geq 1} \mathbb{Z}[1/p](1-p^r)$. Certainly, we have $I_p(U)' \leq I_p(U)^0$, by (4), and to complete the proof it suffices to prove that $e_G - 1 \in I_p(U)'$ for all p-groups. Let G be a non-trivial p-group. We have $e_G = \frac{1}{|G|}\sum_r |G(r)|c_r$ in $X(U)_{\mathbb{Q}}$, the sum being over $1, p, \ldots, p^n$, where G has order p^n. Thus we have $e_G - 1 = \frac{1}{|G|}\sum_{r>1} |G(r)|(c_r - 1)$. Suppose $r > 1$ and $G(r)$ is non-empty. Let k be such that $1 \leq k \leq p-1$ and k is a primitive root of 1 modulo p. A cyclic group A of order $p-1$ with generator a acts on $G(r)$ by $a \cdot x = x^k$. The action is fixed point free and hence $|G(r)|$ is divisible by $p-1$. Hence we get $e_G - 1 \in I_p(U)'$, as required.

We now prove the main result of this section.

(6) *We have:*
(i) $I_p(U)^0 = (p-1)I_p(U)$*; and*
(ii) $I_p(U)$ *is a free* $\mathbb{Z}[1/p]$*-module with basis* $1-c_p, 1-c_{p^2}, \ldots$.

Proof. (i) We have already shown that $I_p(U)^0 \leq (p-1)I_p(U)$, see 3(ii) and the reverse inclusion follows from (1), (3) and (5).
(ii) By §1,(4), the elements $1-c_p, 1-c_{p^2}, \ldots$ linearly independent over $\mathbb{Z}[1/p]$. Hence the elements form a basis over $\mathbb{Z}[1/p]$ by (i) and (5).

3. Global Structure

To complete the picture we prove that the product map $\otimes_p X_p(U) \to X(U)$ is an isomorphism. The main point is that the map is surjective. This is a simple consequence of Brauer's Induction Theorem. However, we prefer a more constructive approach more in keeping with the spirit of this paper. We write $X(U)'$ for the image of the multiplication map $\otimes_p X_p(U) \to X(U)$. By §1,(2), it suffices to show that $e_G \in X(U)'$, for every finite group G. We shall do this by a counting argument which involves regarding the finite group G as a simplicial complex.

Let Δ be a finite simplicial complex. We write Δ_r for the set of r-simplices (i.e. sets σ in Δ with cardinality $|\sigma|$ equal to $r+1$). Let $\mathbb{Z}\Delta$ be the free abelian group with basis Δ. For $\sigma \in \Delta$ we define $\tilde{\sigma} = \sum_{\theta \subseteq \sigma} (-1)^{|\sigma|-|\theta|}\theta \in \mathbb{Z}\Delta$. The following is elementary.

(1) $\sum_{\sigma\in\Delta} \sigma = \sum_{\sigma\in\Delta} N(\sigma)\tilde{\sigma}$, *where* $N(\sigma)$ *is the number of* $\theta \in \Delta$ *such that* $\sigma \subseteq \theta$. *Moreover, we have* $\sum_{\sigma} (-1)^{|\sigma|} N(\sigma) = -|\Delta|$.

We now fix a finite group G. We let X be the subset of G consisting of all non-identity elements of prime power order. We form a simplicial complex Δ on X. A subset of X consisting of elements $x_1, x_2, \ldots, x_r$ is a simplex if x_i is a p_i-element, $1 \leq i \leq r$, for distinct primes $p_1, p_2, \ldots, p_r$ and $x_i x_j = x_j x_i$ for all $1 \leq i, j \leq r$. Thus there is a natural bijection from Δ to $G^\sharp = G \backslash \{1\}$ taking a simplex $\{x_1, \ldots, x_r\}$ to the product $x_1 x_2 \ldots x_r$. We will identity a non-identity element of G with a simplex via this bijection. We note that if $x \in G^\sharp$ and π is the set of primes dividing the order of x then for $y \in G^\sharp$ we have $x \subseteq y$ if and only if x is the π-part of y.

If π is a set of primes we write π' for the complementary set of primes.

(2) *Let* $x \in G^\sharp$ *and let* π *be the set of primes dividing the order of* x. *Then* $N(x)$ *is divisible by the* π' *part of the order of* $Z_G(x)$.

Proof. $N(x)$ is the cardinality of the set $A(x)$ of all $y \in G^\sharp$ with π-part equal to x. An element of $A(x)$ has the form xz, where z is a π' element of the centralizer of x. Hence $N(x)$ is the number of π'-elements contained in the centralizer $Z_G(x)$ of x. Let n be the π'-part of the order of $Z_G(x)$. Then by a theorem of Frobenius (see e.g. [1] or [3]) the number of π' elements in $Z_G(x)$ is a multiple of n.

We write $X(U)'$ for the subring of $X(U)$ generated by the subrings $X_p(U)$, as p ranges over all primes. We introduce an element $\tilde{c}_n \in X(U)$, for each positive integer n. We set $c_1 = 1$. For $n > 1$ we write n as a product $n = q_1 q_2 \ldots q_r$ where $q_i > 1$ is a power of a prime p_i for $1 \leq i \leq r$ and the primes $p_1, p_2, \ldots p_r$ are distinct. We $\tilde{c}_n = (c_{q_1} - 1)(c_{q_2} - 1)\ldots(c_{q_r} - 1)$. Now for positive integers $t_1, t_2, \ldots, t_r$ we have $\frac{1}{q_1^{t_1}}(c_{q_1} - 1) \in X_{p_1}(U)$, $\frac{1}{q_2^{t_2}}(c_{q_2} - 1) \in X_{p_2}(U), \ldots, \frac{1}{q_r^{t_r}}(c_{q_r} - 1) \in X_{p_r}(U)$. Hence we have $\frac{1}{q_1^{t_1} q_2^{t_2} \ldots q_r^{t_r}} \tilde{c}_n \in X(U)'$. Hence we get $\mathbb{Z}[1/n]\tilde{c}_n \in X(U)'$.

We define a linear map $f : \mathbb{Q}U \to X(U)_{\mathbb{Q}}$ by $f(x) = c_n$, where n is the order of x.

Let G be a subgroup of U. Let $1 \neq x \in G$ and write $x = x_1 x_2 \dots x_r$, where $x_1, x_2, \dots, x_r$ are commuting elements of prime power orders $q_1, q_2, \dots, q_r$, where $q_1, q_2, \dots, q_r$ are powers of distinct primes $p_1, p_2, \dots, p_r$. For I a subset of $\{1, 2, \dots, r\}$ we set x to be the product of the elements x_{q_i} with $i \in I$. Then we have $\tilde{x} = (-1)^r \sum_I (-1)^{|I|} x_I$, where the sum is over all non-empty subsets of $\{1, 2, \dots, r\}$. Hence we have $f(\tilde{x}) = \tilde{c}_n - (-1)^{|x|}$, where $|x|$ is the number r of prime divisors of the order n of x.

By §1,(3), we have

$$|G| e_G = 1 + f(\sum_{x \in G^\sharp} x) = 1 + f(\sum_{x \in G^\sharp} N(x)(\tilde{x} + (-1)^{|x|}) - \sum_{x \in G^\sharp} (-1)^{|x|} N(x)$$

and since, by (1), we have $-\sum_{x \in G^\sharp} (-1)^{|x|} N(x) = |G| - 1$, we obtain

$$e_G - 1 = \sum_{x \in G^\sharp} \frac{N(x)}{|G|} f(\tilde{x} + (-1)^{|x|}).$$

For $x \in G^\sharp$ we write $\alpha(x)$ for the order of x. Hence we have

$$e_G - 1 = \sum_{x \in G^\sharp} \frac{N(x)}{|G|} \tilde{c}_{\alpha(x)}.$$

Let the conjugacy classes of non-identity elements of $G^\sharp$ be $C_1, C_2, \dots, C_m$ and choose $g_i \in C_i$, for $1 \leq i \leq m$. Then we have

$$e_G - 1 = \sum_{i=1}^{m} (\sum_{x \in C_i} \frac{N(x)}{|G|} \tilde{c}_{\alpha(x)}) = \sum_{i=1}^{m} \frac{N(g_i)}{|Z_G(g_i)|} \tilde{c}_{\alpha(g_i)} \qquad (*).$$

Now, by (2), for any $1 \neq g \in G$, the quotient $N(g)/|Z_G(g)|$, has the form a/b, where a, b are non-zero integers and b is divisible only by the prime divisors of the order of g. Hence $N(g)/|Z_G(g)| \in \mathbb{Z}[1/n]$, where n is the order of g. Hence, from (*), we have $e_G - 1 \in \sum_{n=1}^{\infty} \mathbb{Z}[1/n] \tilde{c}_n$, i.e. $e_G - 1 \in X(U)'$. This shows that the map $\otimes_p X_p(U) \to X(U)$ in then theorem below is surjective. The remainder follows from the fact that the elements $\tilde{c}_1, \tilde{c}_2, \dots$ form a $\mathbb{Q}$-basis of $X(U)_{\mathbb{Q}}$ (and this follows from the fact the elements $c_1, c_2, \dots$ form a $\mathbb{Q}$-basis).

Theorem (i) Multiplication $\otimes_p X_p(U) \to X(U)$ is a ring isomorphism (where the tensor product is taken over $\mathbb{Z}$ and p runs over all primes).
(ii) We have $X(U) = \oplus_{n=1}^{\infty} \mathbb{Z}[1/n] \tilde{c}_n$.

References

[1] P. Hall, On a theorem of Frobenius, *Proc. Lond. Math. Soc.* **40**(1936), 468–501.
[2] P. Hall, Some constructions for locally finite groups, *J. Lond, Math. Soc.* **34** (1988), 305-319.
[3] M. Hall, The Theory of Groups, *Macmillan, New York.* 1959