APPLICATIONS OF BURNSIDE RINGS IN ELEMENTARY GROUP THEORY

BY

ANDREAS DRESS, CHRISTIAN SIEBENEICHER
AND TOMOYUKI YOSHIDA

Abstract: This is a report on some of the results which appear in [DSY 90]. A canonical ring homomorphism from the Burnside ring $\Omega(C)$ of a finite cyclic group C into the Burnside ring $\Omega(G)$ of any finite group G of the same order is exhibited and it is shown that many results from elementary finite group theory, in particular those claiming certain congruence relations, are simple consequences of the existence of this map.

Theorem:
Let G be a finite group and let C denote the cyclic group of the same order n. There exists a ring homomorphism

$$\alpha = \alpha(G) : \Omega(C) \longrightarrow \Omega(G)$$

from the Burnside ring $\Omega(C)$ of the cyclic group C into the Burnside ring $\Omega(G)$ of the group G with the following property:

- for every subgroup $U \leq G$ of G and every element $x \in \Omega(C)$ one has

  $$\varphi_U(\alpha(x)) = \varphi_{C_{|U|}}(x)$$

  where $\varphi_U(\alpha(x))$ denotes the number of U–invariant elements in the virtual G–set $\alpha(x)$ and $C_{|U|}$ denotes the unique subgroup of order $|U|$ in C.

Remark:
This theorem gives a precise conceptual interpretation of the observation ([Fr 95], [Hu 67], [Wa 80]) that quite a few elementary, but important results in group theory can be proved by comparing systematically certain group theoretic invariants of a finite group G with the same invariants for the cyclic group C of the same order.

The Burnside ring of a finite group

For a finite group G we define its Burnside ring $\Omega(G)$ to be the Grothendieck ring of finite G–sets. It is generated as an algebra over $\mathbf{Z}$ by the (isomorphism classes of) finite (left) G–sets $X, Y, \ldots$, subject to the following relations:

$$\begin{aligned} X - Y &= 0 \qquad \text{if } X \cong Y, \\ X + Y - (X \dot{\cup} Y) &= 0, \\ X \cdot Y - (X \times Y) &= 0. \end{aligned}$$

The elements of $\Omega(G)$ are the *virtual G–sets*, i. e. , the formal differences $X - Y$ of (isomorphism classes of) finite G–sets X, Y.

Burnside numbers and the associated canonical homomorphisms

Consider now for any G–set X and every subgroup U of the group G the subset

$$X^U := \{x \in X \mid u \cdot x = x \quad \text{for all } u \in U\}$$

of U–invariant elements of X.

The mapping

$$X \mapsto \varphi_U(X) := \# X^U$$

which associates to the G–set X the number of U–invariant elements of X (its *Burnside number* with respect to the subgroup U) extends to a canonical ring homomorphism

$$\varphi_U : \Omega(G) \longrightarrow \mathbf{Z}.$$

Note that in particular one has

$$\varphi_1(X) = \text{cardinality of } X$$

if $1 = \{1_G\}$ denotes the trivial subgroup of G.

Essential properties of the canonical homomorphisms

- For $U, V \leq G$ one has $\varphi_U = \varphi_V$ if and only if U and V are conjugate in G ($U \overset{G}{\sim} V$).
- For $x, x' \in \Omega(G)$ one has $\varphi_U(x) = \varphi_U(x')$ for all $U \leq G$ if and only if $x = x'$.

The canonical injection of the Burnside ring into the ghost ring

Consider for each $x \in \Omega(G)$ to the map

$$U \longmapsto \varphi_U(x)$$

from the set $\mathrm{Sub}(G)$ of all subgroups of G into $\mathbf{Z}$. Then

$$x \mapsto (U \longmapsto \varphi_U(x))$$

provides a canonical homomorphism $\varphi : \Omega(G) \longrightarrow \tilde{\Omega}(G)$ from the Burnside ring into the *ghost ring*

$$\tilde{\Omega}(G) := \mathbf{Z}^{\mathrm{Sub}(G)/\sim}$$

of G, consisting of all maps from $\mathrm{Sub}(G)$ into $\mathbf{Z}$ which are constant on each conjugacy class of subgroups.

This homomorphism is injective and allows to interpret the Burnside ring $\Omega(G)$ as a subring of the ghost ring $\tilde{\Omega}(G)$.

The canonical basis of the Burnside ring

For every subgroup U of the group G one has the G–set $G/U := \{gU \mid g \in G\}$ of left cosets of G modulo U. It is transitive and every transitive G–set is isomorphic to one of this form.

Since every G–set decomposes uniquely into a disjoint union of transitive G–sets, the (isomorphism classes of the) coset spaces G/U form a $\mathbf{Z}$–basis of $\Omega(G)$ and every element $x \in \Omega(G)$ can be expressed as a linear combination in the form

$$x = \sum_{U \leq G}{}' \mu_U(x) \cdot G/U$$

with uniquely determined integral coefficients $\mu_U(x) \in \mathbf{Z}$, satisfying $\mu_U(x) = \mu_V(x)$ for $U \overset{G}{\sim} V$. The prime attached to the summation symbol $\sum'$ indicates that the sum extends only over a system of representatives of the conjugacy classes of subgroups of G.

Calculating Burnside numbers

For every element x of the G–set X denote by $G_x := \{g \in G \mid gx = x\}$ the isotropy group of x.

- If $f : X \longrightarrow Y$ is a G–map mapping the element $x \in X$ to the element $y \in Y$ then $G_x \leq G_y$.
- *Vice versa*:
  If X is a transive G–set and if $G_x \leq G_y$ then there exists a unique G–map mapping x to y.
- This provides a canonical bijection

  $$\mathrm{Hom}_G(G/V, X) \cong X^V \qquad f \mapsto f(V)$$

  which specializes for $Y = G/U$ to

  $$(G/U)^V \cong \mathrm{Hom}_G(G/V, G/U)$$

- Hence:
  $\varphi_V(G/U) \neq 0$ if and only if there exists some element $g \in G$ with $V \subseteq gUg^{-1}$, i. e. if V is sub–conjugate to U ($V \overset{<}{\sim}_G U$).

Note that $\mathrm{Aut}_G(G/U)$ operates freely on G/U and that $\mathrm{Aut}_G(G/U) \cong N_G(U)/U$. Therefore

$$\begin{aligned} \varphi_V(G/U) &= \#\{gU \in G/U \mid VgU = gU\} \\ &= (N_G(U):U) \cdot \#\{U' \leq G \mid V \leq U' \overset{G}{\sim} U\}. \end{aligned}$$

Hence for a given element $x \in \Omega(G)$ a subgroup U of G

- is a *maximal* subgroup with $\mu_U(x) \neq 0$

  if and only if

- it is a *maximal* subgroup with $\varphi_U(x) \neq 0$

and for such a maximal subgroup one has

$$\varphi_U(x) = \mu_U(x) \cdot \varphi_U(G/U) = \mu_U(x) \cdot (N_G(U):U).$$

An application for p–groups

The unique representation

$$x = \sum_{U \leq G}{}' \mu_U(x) \cdot G/U$$

existing for every $x \in \Omega(G)$ implies in case that G is a p–group:

$$\begin{aligned} \varphi_1(x) &= \sum_{U \leq G}{}' \mu_U(x) \cdot (G:U) \\ &\equiv \mu_G(x) = \varphi_G(x) \qquad \pmod{p}. \end{aligned}$$

Corollary:
If V is a p–subgroup of an arbitrary finite group G and if U is a subgroup of G with an index $(G:U)$ which is prime to p, then

$$\varphi_V(G/U) \equiv \varphi_1(G/U) = (G:U) \not\equiv 0 \pmod{p}$$

and therefore V is sub–conjugate to U ($V \overset{<}{\sim}_G U$).

Corollary:
If Sylow p–subgroups exist in G, they all must be *conjugate* in G and every other p–group must be sub–conjugate in G to each of them.

Proof of the Theorem

Let β denote the map from $\mathrm{Sub}(G)$ into $\mathrm{Sub}(C)$ which associates to every subgroup U of G the unique subgroup $C_{|U|}$ of C which has the same number of elements as U. Then clearly, β induces a ring homomorphism

$$\gamma = \gamma(G) : \widetilde{\Omega}(C) \longrightarrow \widetilde{\Omega}(G) \qquad s \longmapsto s \circ \beta$$

from the ghost ring of C into the ghost ring of G such that

$$\varphi_U(\alpha(x)) = \varphi_{C_{|U|}}(x).$$

Hence the Theorem just claims that γ maps the subring $\Omega(C)$ of $\widetilde{\Omega}(C)$ into the subring $\Omega(G)$ of $\widetilde{\Omega}(G)$ and that α is precisely the restriction of γ onto $\Omega(C)$.

To prove that $\gamma(\Omega(C))$ is already contained in $\Omega(G)$ recall that for every finite G–set X and every natural number q the set $\binom{X}{q}$ of all subsets Y of X of cardinality q is also a finite G–set relative to the G–action

$$G \times \binom{X}{q} \longrightarrow \binom{X}{q} : (g, Y) \longmapsto g \cdot Y := \{g \cdot y \mid y \in Y\}.$$

Using these G–sets for the *regular* G–set $X := G/1$ the Theorem follows immediately from the following two observations:

Lemma 1:
γ maps $\binom{C/1}{q} \in \Omega(C) \subseteq \widetilde{\Omega}(C)$ onto $\binom{G/1}{q} \in \Omega(G) \subseteq \widetilde{\Omega}(G)$.

Lemma 2:
If $J_n := \{d \in \mathbf{N} \mid d \text{ divides } n\}$ denotes the set of divisors of n then the family $\binom{C/1}{d}$ $(d \in J_n)$ of C–sets forms a $\mathbf{Z}$–basis of $\Omega(C)$.

Lemma 1 in turn is an immediate consequence of the well–known fact that the Burnside number $\varphi_U(\binom{G/1}{q})$, that is, the number of U–invariant subsets of cardinality q in $G/1$, depends only on q and the orders of G and of U. This fact is expressed more explicitly in the following

Lemma 1′:

For every finite group G, every subgroup U of G, and every $q \in \mathbf{N}$ one has

$$\varphi_U(\binom{G/1}{q}) = \begin{cases} 0 & \text{if } |U| \text{ does not divide } q, \\ \binom{(G:U)}{q/|U|} & \text{otherwise,} \end{cases}$$

In particular, if $|U| = q$, then

$\varphi_U(\binom{G/1}{q}) = (G:U)$ and therefore

$$\mu_U(\binom{G/1}{q}) = \frac{(G:U)}{(N_G(U):U)} = (G:N_G(U)).$$

Proof of Lemma 1′:

- $Y \in \binom{G/1}{q}$ is U–invariant if and only if Y is the union of right cosets $Ug \subseteq G$ of U in G.
- Hence such a subset Y exists only if $|U|$ divides q.
- In this case the set $\binom{G/1}{q}^U$ of U–invariant subsets Y in $\binom{G/1}{q}$ corresponds in a one–to–one fashion to the set $\binom{U\backslash G}{q/|U|}$ of subsets of $U\backslash G := \{Ug \mid g \in G\}$ of cardinality $q/|U|$.
- So its cardinality is of course $\binom{(G:U)}{q/|U|}$, as stated.

Proof of Lemma 2:

For every $d, d' \in J_n$ we have integers

$$\mu_{d,d'} = \mu_{C_{d'}}(\binom{C/1}{d}) \in \mathbf{Z}$$

such that

$$\binom{C/1}{d} = \sum_{d' \in J_n} \mu_{d,d'} \cdot C/C_{d'}$$

and we have to show that the determinant of the matrix

$$M := (\mu_{d,d'})_{d,\, d' \,\in\, J_n}$$

is a unit in $\mathbf{Z}$.

In view of Lemma 1 we have

- $\varphi_{C_{d'}}(\binom{C/1}{d}) = 0$ unless d' divides d.
- Hence, we have also $\mu_{d,d'} = 0$ unless d' divides d.
- Therefore M is a *triangular* Matrix (relative to the obvious ordering of J_n according to which d comes before d' if d is smaller than d').
- In addition, we have

  $$\mu_{d,d} = \mu_{C_d}(\binom{C/1}{d}) = (C : N_C(C_d)) = 1,$$

  so the main diagonal of M consists of one's, only.

Hence the determinant of the matrix M is indeed equal to 1.

Remark:
Rather than using *exterior powers* of G–sets, that is, the G–sets of the form $\binom{G/1}{q}$, introduced by H. Wielandt [Wi 59]] in this context, we could as well have used the *symmetric powers*, that is, the G–sets of the form

$$S^q(X) := \{f : X \longrightarrow \mathbf{N}_0 \mid \sum_{x\in X} f(x) = q\},$$

used by B. Wagner [Wa 80]. As before, the value of $\varphi_U(S^q(G/1))$ depends only on q, $|G|$, and $|U|$ and vanishes unless $|U|$ divides q, and the family $S^d(C/1) \quad (d \in J_n)$ of C–sets forms a $\mathbf{Z}$–basis of $\Omega(G)$.

Corollary 1:
For every divisor d of $|G|$ there exists an element $x_d \in \Omega(G)$ satisfying

$$\varphi_U(x_d) = \begin{cases} d & \text{if } d \text{ divides } (G:U), \\ 0 & \text{otherwise,} \end{cases}$$

In particular, $\mu_U(x_d) = 0$ unless d divides $(G : U)$ and

$$\mu_U(x_d) = (G : N_G(U)) = \#\{gUg^{-1} \mid g \in G\}$$

if $(G : U) = d$.

Proof of Corollary 1:
Put $x_d := \alpha(C/C_{|G|/d})$. Then one has

- $\varphi_U(x_d) = \varphi_{C_{|U|}}(C/C_{|G|/d}) = (C : C_{|G|/d}) = d$ if $C_{|U|} \subset C_{|G|/d}$ that is, if the index d of $C_{|G|/d}$ in C divides the index $(C : C_{|U|}) = (G : U)$ of $C_{|U|}$ in C.

- $\varphi_U(x_d) = 0$ otherwise and therefore also $\mu_U(x_d) = 0$ if d does not divide $(G : U)$.

- If $(G : U) = d$, then U is a maximal subgroup of G with $\mu_U(x_d) \neq 0$ and therefore

$$\begin{aligned}\mu_U(x_d) &= \frac{\varphi_U(x_d)}{(N_G(U):U)} = \frac{d}{(N_G(U):U)} \\ &= \frac{(G:U)}{(N_G(U):U)} = (G : N_G(U))\end{aligned}$$

  equals the number of subgroups in G which are conjugate to U in G.

To derive the next three corollaries we follow essentially the ideas of B. Wagner [Wa 80].

Corollary 2 (Sylow):

Every divisor d of $|G|$ is the greatest common divisor of all indices $(G : U)$ of subgroups U in G which are divisible by d, that is, we have

$$d = \text{g.c.d.}\,(\,(G:U) \mid d \text{ divides } (G:U))\,.$$

In particular (or, as well, equivalently),

- if $|G| = d \cdot p^\alpha$ for some prime p, then there exist subgroups U of G of index d and hence of order p^α.

In case $|G|/d$ is a power of a prime p we can exploit this argument even further to derive:

Corollary 3 (Sylow, Frobenius):

If a power p^α of a prime p divides the order $|G|$ of a finite group G, then the number of subgroups V of order p^α is congruent to 1 modulo p.

Proof of Corollary 2:
Write $x_d \in \Omega(G)$ in the form

$$x_d = {\sum_{U \leq G}}' \mu_U(x_d) \cdot G/U = {\sum_{U \leq G,\, d|(G:U)}}' \mu_U(x_d) \cdot G/U$$

and apply φ_1 to derive

$$d = {\sum_{U \leq G, d|(G:U)}}' \mu_U(x_d) \cdot (G:U)$$

and consequently

$$d \in {\sum_{U \leq G, d|(G:U)}}' \mathbf{Z} \cdot (G:U).$$

Proof of Corollary 3:
Put $d := |G|/p^\alpha$ and divide the above equation

$$\begin{aligned} d &= {\sum_{U \leq G,\, d|(G:U)}}' \mu_U(x_d) \cdot (G:U) \\ &= {\sum_{U \leq G,\, |U| \in J_{p^\alpha}}}' \mu_U(x_d) \cdot (G:U) \end{aligned}$$

by d to derive

$$\begin{aligned} 1 &= {\sum_{U \leq G, d|(G:U)}}' \mu_U(x_d) \cdot \frac{(G:U)}{d} \\ &= {\sum_{U \leq G, |U| \in J_{p^\alpha}}}' \mu_U(x_d) \cdot \frac{p^\alpha}{|U|} \\ &\equiv {\sum_{U \leq G, |U| = p^\alpha}}' \mu_U(x_d) \\ &= {\sum_{U \leq G, |U| = p^\alpha}}' (G : N_G(U)) \\ &= {\sum_{U \leq G, |U| = p^\alpha}}' \#\{gUg^{-1} \mid g \in G\} \\ &= \#\{V \leq G \mid |V| = p^\alpha\} \qquad \pmod{p}. \end{aligned}$$

Cauchy–Frobenius–Burnside congruence relations

To derive the next corollary let us recall that for every $x \in \Omega(G)$ one has the so called

Cauchy–Frobenius–Burnside congruence relation

$$\sum_{g\in G} \varphi_{\langle g\rangle}(x) \quad \equiv \quad 0 \pmod{|G|}.$$

By additivity it is enough to verify this just for $x = G/U$ $(U \leq G)$ in which case a standard computation yields

$$\begin{aligned}
\sum_{g\in G} \varphi_{\langle g\rangle}(G/U) &= \sum_{g\in G} \#\{hU \in G/U \mid ghU = hU\} \\
&= \sum_{hU\in G/U} \#\{g \in G \mid ghU = hU\} \\
&= \sum_{hU\in G/U} |hUh^{-1}| \\
&= (G:U)\cdot|U| = |G| \\
&\equiv 0 \pmod{|G|}.
\end{aligned}$$

with the Cauchy–Frobenius–Burnside relation Corollary 1 yields

Corollary 4 (Frobenius):

Every divisor m of the order $|G|$ of a finite group G divides also the number

$$\#\{g \in G \mid g^m = 1\}$$

of elements g in G, whose order divides m.

Proof:

Apply the Cauchy–Frobenius–Burnside congruence relation to x_d for $d := |G|/m$ to derive that $|G| = d\cdot m$ divides

$$\begin{aligned}
\sum_{g\in G} \varphi_{\langle g\rangle}(x_d) &= \sum_{g\in G, d|(G:\langle g\rangle)} d \\
&= \sum_{g\in G, |g|\in J_m} d \\
&= d\cdot\#\{g \in G \mid g^m = 1\}
\end{aligned}$$

and hence, dividing by d, that m divides $\#\{g \in G \mid g^m = 1\}$.

For more details, further applications and detailed references see [DSY 90].

References

[DSY 90] DRESS (A. W. M.), SIEBENEICHER (CH.), YOSHIDA (T.) — *An Application of Burnside Rings in Elementary Finite Group Theory* — Preprint 90–033 des SFB 343 Diskrete Strukturen in der Mathematik, Bielefeld 1990, to appear in Adv. in Math.

[Fr 95] FROBENIUS (G.) — *Verallgemeinerung des Sylowschen Satzes* — Sitzungsberichte der Königlich Preußischen Akademie der Wissenschaften zu Berlin (1895) 981–993, in *Gesammelte Abhandlungen* Bd. II, Springer–Verlag, Berlin–New York, 1968, 664–676.

[Fr 03] FROBENIUS (G.) — *Über einen Fundamentalsatz der Gruppentheorie* — Sitzungsberichte der Königlich Preußischen Akademie der Wissenschaften zu Berlin (1903) 987–991, in *Gesammelte Abhandlungen* Bd. III, Springer–Verlag, Berlin–New York, 1968, 330–334.

[Fr 07] FROBENIUS (G.) — *Über einen Fundamentalsatz der Gruppentheorie* — Sitzungsberichte der Königlich Preußischen Akademie der Wissenschaften zu Berlin (1907) 428–437, in *Gesammelte Abhandlungen* Bd. III, Springer–Verlag, Berlin–New York, 1968, 428–437.

[Hu 67] HUPPERT (B.) — Endliche Gruppen I — Springer Verlag, Berlin–Heidelberg–New York, 1967, p. 34.

[Sy 72] SYLOW (L.) — *Théorèmes sur les groupes de substitutions* — Math. Ann., **5** (1872), 584–594.

[Wa 80] WAGNER (B.) — *A permutation representation theoretical version of a theorem of Frobenius* — Bayreuther Mathematische Schriften **6** (1980), 23–32.

[Wi 59] WIELANDT (H.) — *Ein Beweis für die Existenz der Sylowgruppen* — Arch. der Math., **10** (1959), 401 – 402.