Demonstration of the Fermat’s Little Theorem in Context of the Burnside Rings

Kenneth K. Nwabueze

Department of Mathematics, Faculty of Science, Universiti Brunei Darussalam, BE 1410, Gadong, Brunei nwabueze@fos.ubd.edu.bn, kknwabueze@hotmail.com

Abstract

We demonstrate proof of the Fermat’s little theorem in the context of the Burnside ring.

1 The Burnside ring of finite groups

The Burnside ring \( B(G) \) of a finite group \( G \) is the Grothendieck ring of finite \( G \)-sets. It is generated as an algebra over \( \mathbb{Z} \) by the isomorphism classes of finite (left) \( G \)-sets \( S, T, \cdots \), subject to the relations

\[
\begin{align*}
S - T &= 0, \text{ if } S \cong T, \\
S + T - (S \cup T) &= 0, \\
S \cdot T - (S \times T) &= 0
\end{align*}
\]

Therefore, the elements of \( B(G) \) are the virtual \( G \)-sets; that is, the formal differences \( S - T \) of isomorphism classes of \( G \)-sets \( S, T \); (see [1], [3]). For reader’s convenience, we start by writing down some of the notations used in this paper.

**Notation 1.1** Let \( H, K \) be subgroups of a finite group \( G \). We say that \( H \) and \( K \) are \( G \)-conjugate and write \( H \sim_G K \) if \( g^{-1}Hg = K \) for some \( g \in G \). If \( g^{-1}Hg \subseteq K \) for some \( g \in G \), we write \( H \preceq_G K \), and say that \( H \) is \( G \)-subconjugate to \( K \). We denote the set of \( G \)-invariant subset of a \( G \)-set \( S \) by

\[
\text{Fix}_G(S) := \{ s \in S \mid gs = s \ \forall \ g \in G \};
\]

in particular, for \( K \leq G \), we have that

\[
\text{Fix}_H(G/K) = \{ gK \mid g \in G, \ g^{-1}Hg \leq K \}.
\]
The following results are well known (see [1], [3]).

**Proposition 1.1** Let \( H \) and \( K \) be subgroups of \( G \), and let \( S \) be any \( G \)-set. Then

(i) there exists a bijection \( \text{Hom}_G(G/H, G/K) \leftrightarrow \text{Fix}_H(S) \),

(ii) there exists a bijection \( \text{Hom}_G(G/H, G/K) \leftrightarrow \text{Fix}_H(G/K) \),

(iii) \( \text{Fix}_H(G/K) = \emptyset \) unless \( G \unlhd K \),

(iv) \( G/H \cong G/K \) as \( G \)-sets if and only if \( H \sim G K \).

The above proposition implies that if \( S = S(G) \) is a full set of nonconjugate subgroups of \( G \), then the \( G \)-sets \( \{ G/H \mid H \in S \} \) form a \( \mathbb{Z} \)-basis of \( B(G) \), that is

\[
B(G) = \sum_{H \in S} \mathbb{Z} [G/H].
\]

Furthermore, for every subgroup \( H \) of \( G \), the \( G \)-set \( G/H \) is transitive and every transitive \( G \)-set is isomorphic to one of this form. Now, because every \( G \)-set decomposes uniquely into a disjoint union of transitive \( G \)-sets, every element \( [S] \in B(G) \) can be written as a linear combination of the form

\[
[S] = \sum_{H \leq G} m_H([S])G/H
\]

with uniquely determined integral coefficients \( m_H[S] \in \mathbb{Z} \), satisfying \( m_H([S]) = m_K([S]) \) if \( H \unlhd G K \).

2 A canonical homomorphism

If \( S \) and \( T \) are \( G \)-sets, then clearly we have for every subgroup \( H \leq G \), that

\[
\text{Fix}_H(S \cup T) = \text{Fix}_H(S) \cup \text{Fix}_H(T),
\]

\[
\text{Fix}_H(S \times T) = \text{Fix}_H(S) \times \text{Fix}_H(T).
\]

Therefore, we can define a ring homomorphism

\[
\phi_H := \{ \phi_H \mid H \leq G \} : B(G) \to \mathbb{Z}
\]

induced by the map

\[
S \to \phi_H(S) := |\text{Fix}_H(S)|.
\]

\(^{1}\)we have used the summation symbol in the form \( \sum' \) (that is, with a prime attached) to indicate that the sum extends only over a system of representatives of conjugacy classes of subgroups of \( G \).
Furthermore, if $H$ and $K$ are $G$-conjugate then $\phi_H = \phi_K$ because if $g \in G$ and $S$ is any $G$-set then $s \in Fix_H(S)$ if and only if $gs \in Fix_{gHg^{-1}}(S)$. Note that for the trivial subgroup $1_G := 1$ of $G$, we have

$$\phi_1(S) = \text{cardinality of } S.$$ 

If we put $K = H$ in proposition 1.1(ii), we get

$$\phi_H[G/H] = |N_G(H) : H|,$$

where $N_G(H)$ is the normalizer of $H$ in $G$.

## 3 The ghost ring

The following well known result (see [3]) shows that the set of ring homomorphisms $\phi_H$ from $B(G)$ to $\mathbb{Z}$ distinguish the elements of the Burnside ring $B(G)$ from one another.

**Theorem 3.1** Let $S,T$ be $G$-sets, and let $S$ be a full set of nonconjugate subgroups of $G$. Then $S \cong T$ if and only if $\phi_H(S) = \phi_H(T)$ for all $H \in S$.

Observe that for each $[S] \in B(G)$, the map $H \to (H \to \phi_H([S]))$ from the set of subgroups of $G$ into $\mathbb{Z}$ induces a homomorphism

$$\phi_H : B(G) \to \tilde{B}(G) : [S] \to (H \to \phi_H([S]))$$

from the Burnside ring $B(G)$ into its *ghost ring*

$$\tilde{B}(G) := \mathbb{Z}^{\mathbb{S}/\sim}$$

of $G$, consisting of all maps from all subgroups of $G$ into $\mathbb{Z}$ which are constant on each conjugacy class of subgroups of $G$. It is obvious that this homomorphism is injective [3] and so we can regard the Burnside ring $B(G)$, in a canonical way, as a subring of the ghost ring $\tilde{B}(G)$.

## 4 Cauchy-Frobenius-Burnside relations

The following result, called the Cauchy-Frobenius-Burnside relations is well known [3].

**Theorem 4.1** Let $G$ be a finite group. Then for every $[S] \in B(G)$, we have the congruence relation

$$\sum_{g \in G} \phi_{\langle g \rangle}([S]) \equiv 0 \pmod{|G|}.$$
Finally, note that because we have the unique representation

\[ [S] = \sum_{H \leq G} m_H([S])G/H \]

for every \([S] \in B(G)\), it follows that in the case where \(G\) is a \(p\)-group, we have

\[ \phi_1([S]) = \sum_{H \leq G} m_H([S])\phi_H(G/H) \equiv m_G([S]) = \phi_G([S]) \pmod p. \]

5 Fermat’s Little theorem

The Fermat little theorem (see [2]) is the statement of the next theorem and we now demonstrate its proof using the Burnside ring oriented approach.

**Theorem 5.1 (Fermat):** Let \(n \geq 1\) be any integer and \(p\) a prime. Then \(n^p \equiv n \pmod p\).

**Proof:** Let \(G\) denote a cyclic group of order \(p\), and for \(n \in \mathbb{N} (n \geq 1)\), let \(N := \{1, \ldots, n\}\) be a set of integers from 1 to \(n\). Set \(S = N^p\), and let \(G\) act on \(S\) by cyclic permutation of entries of an element in \(S\). It is obvious that \(S\) with this action is a \(G\)-set of cardinality \(n^p\). Furthermore \((a_1, a_2, \cdots a_p) \in S\) is in \(Fix_G(S)\) if and only if \(a_1 = a_2 = \cdots = a_p\); and so \(|Fix_G(S)| = n\). Write \([S] = \sum_{H \leq G} n_H G/H\). Now we apply \(\phi_1\) to \([S]\) to derive

\[ n^p = \phi_1([S]) = \phi_1 \left( \sum_{H \leq G} n_H([S])G/H \right) = \sum_{H \leq G} n_H([S])(G : H) \equiv n_G([S]) = \phi_G([S]) \pmod p = n \pmod p. \]

That is, \(n^p \equiv n \pmod p\) for all \(n \in \mathbb{N}\). Now, because \((-1)^p \equiv -n^p\), we have that \(n^p \equiv n \pmod p\) for all \(n \in \mathbb{Z}\).

**Corollary 5.1** If \(n \geq 1\) is an integer and \(p\) a prime, then \(n^{p^k} \equiv n \pmod p\) for all \(k \geq 1\).

**Proof:** Repeat the argument in the proof of theorem 5.1, by setting \(S = N^{p^k}\) and allowing a cyclic group of order \(p^k\) to act cyclically on \(S\).
References


Received: August 7, 2007