A CANCELLATION THEOREM
CHAPTER VI

A CANCELLATION THEOREM

6.1. INTRODUCTION: As we have seen in our previous chapters, some ring-theoretic analogues of simple group-theoretic results concerning commutativity are established very late [42]. It seems surprising that the ring-theoretic versions of many other well-known group-theoretic results still escaped the attention of the research workers. The reason for this sort of omission is understandable. We know that the essential mechanism in the proofs of almost all such results in groups is cancellation, which is not permissible in general class of rings. Only a few results could be proved by going through several steps of permutations of the substitutions like \( y \) by \( x+y \) and \( x \) by \( x+1 \) starting with the given identity, while to obtain some more results very complicated combinatorial arguments (to say, [6], [21]) had to be used. In this chapter we obtain a theorem which allows a limited cancellation in rings with unity. In the last section of the chapter we use our theorem to easily deduce a number of commutativity theorems.

6.2. Though over the last three or four decades, a great deal of work was done which showed that under certain types of hypothesis rings had to be commutative, but surprisingly many simple results like one obtained by Johnsen, Outcalt and Yaqub [42] in 1968, did not catch attention of the researchers, working in this domain. The reason is simple that the cancellation is essentially not permissible in rings. In this section we attempt to obtain a theorem which allows us a sort of cancellation in rings and thus helps us derive easily many commutativity theorems.

The proof of the theorem depends on the simple strategy to substitute say, \( x+1 \) for \( x \) to get another identity simpler than the original one.
Let $R[X,Y,Z]$ denote the ring of the polynomials in noncommuting indeterminates $X, Y, Z$ over $R$. Define an automorphism $\sigma$ on $R[X,Y,Z]$ by:

1. $\sigma[F(X,Y,Z)] = F(X+1,Y,Z)$

and a $\sigma$-derivation $\Delta = \sigma - I$:

2. $\Delta[F(X,Y,Z)] = F(X+1,Y,Z) - F(X,Y,Z)$

Easy computations show that for any two polynomials $F = F(X,Y,Z)$ and $G = G(X,Y,Z)$ in $R[X,Y,Z]$, we have

3. $\Delta[F+G] = \Delta[F] + \Delta[G]$

4. $\Delta[FG] = (\Delta[F])(\sigma[G]) + F(\Delta[G])$

and an induction give the Leibniz formula

5. $\Delta^n[FG] = \sum_{r=0}^{n} \binom{n}{r} (\Delta^r[F])(\sigma^r\Delta^{n-r}[G])$

This allows us to prove:

**Lemma 6.2.1:** If $F$ is homogeneous of degree $n$ in $X$, then $\Delta^n[F(X,Y,Z)] = n!F(1,Y,Z)$ and $\Delta^m[F(X,Y,Z)] = 0$ for $m > n$.

**Proof:** By (3) it suffices to prove the lemma when $F(X,Y,Z)$ is a monomial. It can be proved by induction on $n$. If $n = 0$, $F(X,Y,Z)$ is independent of $X$ and $\Delta^0[F(X,Y,Z)] = F(X,Y,Z) = F(1,Y,Z)$. Again $\Delta[F(X,Y,Z)] = F(X+1,Y,Z) - F(X,Y,Z) = 0$ and hence $\Delta^m[F(X,Y,Z)] = 0$ for all $m > 0$.

For induction step, write the monomial $F(X,Y,Z)$ as $AXG$ where $A$ is a monomial with no $X$'s in it and $G$ is a monomial of degree $n-1$ in $X$. Then $\Delta[A] = 0$ and by (4), $\Delta[AX] = A$; hence $\Delta^r[AX] = \Delta^{r-1}[A] = 0$ for $r > 1$ by the case $n = 0$. Again by using (5), we get

$$\Delta^m[AXG] = (AX) \Delta^m[G] + nA (\sigma \Delta^{m-1}[G])$$
By the induction hypothesis the first term on the right side is zero if \( m \geq n \). The second term is zero if \( m > n \); if \( m = n \) then

\[ nA(n-1)!G(1,Y,Z) = n!F(1,Y,Z), \]

which proves the lemma.||

Now we are ready to prove the following theorem:

**THEOREM 6.2.1:** Let \( R \) be an associative ring with unity \( 1 \) and let \( F(X,Y,Z) \) be a polynomial with coefficients from elements of \( R \) where the indeterminates commute neither with each other nor with the elements of \( R \). Suppose that \( F \) is homogeneous in \( X \) of degree \( n \) and homogeneous in \( Y \) of degree \( m \) and that \( F(x,y,xy-yx)=0 \) for all \( x \) and \( y \) in \( R \). Then \( m!n!F(1,1,xy-yx)=0 \) for all \( x \) and \( y \) in \( R \).

**PROOF:** If \( F(x,y,xy-yx) = 0 \) for all \( x \) and \( y \) in \( R \), then on replacing \( x \) by \( x+1 \), we get

\[ F(x+1,y,(x+1)y-y(x+1)) = F(x+1,y,xy-yx) = 0 \]

That is, if \( F(x,y,xy-yx) \) is identically zero, the same is true for \( \sigma[F] \), \( \Delta[F] \) and \( \Delta^n[F] \). Hence \( n!F(1,y,xy-yx) = 0 \) for all \( x \) and \( y \) in \( R \). Now apply the whole procedure again on the polynomial \( F(1,Y,Z) \) which is homogeneous of degree \( m \) in \( Y \) by using a new derivation \( \Delta' \) defined as

\[ \Delta'[F(X,Y,Z)] = F(1,Y+1,Z) - F(Y,Z) \]

The result is the conclusion of the theorem.||

6.3. APPLICATIONS TO COMMUTATIVITY THEOREMS: We can drive a number of results with the help of our theorem proved above. Even those results ([6],[21]), which were proved earlier by using very complicated combinatorial arguments will become corollaries of our theorem. We need just to select a suitable polynomial \( F(X,Y,Z) \).

Let us assume hence onward that \( R \) is an associative ring with Unity \( 1 \).
We begin to prove the following result due to Johnsen, Outcalt and Yaqub [42].

THEOREM 6.3.2: Let $R$ be a ring satisfying $(xy)^2 = x^2y^2$ for all $x,y$ in $R$. Then $R$ is commutative.

PROOF: If $F(X,Y,Z) = XZY$, then indeed $F(x,y,xy-yx) = x^2y^2 - (xy)^2 = 0$ hence by applying Theorem 6.2.1, $F(1,1,xy-yx) = 0$ i.e. $xy-yx = 0$ and ring $R$ is commutative. ||

The noncommutative ring of Example 5.2.1 for $p = 3$ shows that, if we replace $(xy)^2 = x^2y^2$ by the identity $(xy)^3 = x^3y^3$ in the hypothesis of the above theorem, then the result fails. We notice that the characteristic of this ring is 3. Does the characteristic of the ring play any role in the commutativity, if the ring satisfies $(xy)^3 = x^3y^3$? In the following theorem we attempt to settle the question, posed above.

THEOREM 6.3.3: Let $R$ be a ring satisfying $(xy)^3 = x^3y^3$ for all $x,y$ in $R$. If characteristic of $R$ is neither 2 nor 3, then $R$ is commutative.

PROOF: Take $F(X,Y,Z) = X^2YZ + XZXY + XYXZ$, then $F(x,y,xy-yx) = x^3y^3 - (xy)^3 = 0$ and by our Theorem 6.2.1, $2!2!1F(1,1,xy-yx) = 2!2!3(xy-yx) = 0$. But 2 and 3 are not zero divisors in $R$ so $xy-yx = 0$ which gives commutativity. ||

In fact applying Theorem 6.2.1, we can derive even more general results. As an example we prove below a generalization of Theorem 6.3.2, which was earlier established by Awtar [6].

THEOREM 6.3.4: Let $n > 1$ be a positive integer and $R$ be a ring of not characteristic $p$ for every prime $p \leq n$. If $R$ satisfies $(xy)^n = x^ny^n$ for all $x$ and $y$ in $R$, then $R$ is commutative.
PROOF: Just as we did in proof of Theorem 6.3.3, we take $F(X,Y,Z)$ to be a sum of $n(n-1)/2$ monomials each of which is a product of one $Z$ by $n-1$ $X$'s and $n-1$ $Y$'s (it takes one term to move each $Y$ in $XYXY$ to the right, past one $X$). Then we have $F(x,y,xy-yx) = x^n y^n - (xy)^n$ and by Theorem 6.2.1, the above remarks yield that

$$m!n! F(1,1, xy-yx) = ((n-1)!)^2(n(n-1)/2)(xy-yx) = 0$$

which implies that $xy-yx = 0$ if all primes dividing $((n-1)!)^2(n(n-1)/2)$ are not zero divisors in $R$.||

If we choose the polynomial $F(X,Y,Z) = XYZ + ZYX$, then we get the following result which is a particular generalization of a theorem of Belluce, Herstein and Jain [12], for the case $m=n=2$.

THEOREM 6.3.5: Let $R$ be a ring satisfying $(xy)^2 = (yx)^2$ for all $x,y$ in $R$. If the additive group of $R$ has no element of order 2, then $R$ is commutative.

REMARKS 1. If we take $F(X,Y,Z) = ZXY$, the polynomial identity

$$(xy)^2 - yx^2 y = 0$$

or if $F(X,Y,Z) = XYZ$, then the polynomial identity

$$(xy)^2 - xy^2 x = 0$$

implies commutativity which is of course Theorem 5.2.1.

2. Similarly if $F(X,Y,Z) = YZX + YXZ + ZXY$, then the polynomial identity

$$(xy)^2 - y^2 x^2 = 0$$

implies commutativity provided the additive group of the ring $R$ has no element of order 3.

3. If we consider $F(X,Y,Z) = XZ - 2ZY$, the polynomial identity

$$(x+2y)xy = xy (x+2y)$$

for all $x,y$ in $R$ renders the ring $R$ commutative.

Other examples can be constructed ad libitum, ad infinitum.

4. More subtle commutativity theorems, which do not work for all rings with unity, also often assume polynomial identities of the form

$F(x,y,xy-yx) = 0$ but with $F(1,1,xy-yx) = 0$. 