

The same thing also applies the last step.
By XOR'ing the blend with b (which is a 's original value now) we set b 's original value and assign it to a .

THE ALGEBRAIC PROOF:

Operations:

1. $a = a \oplus b$

2. $b = a \oplus b$

3. $a = a \oplus b$

So that a is now the blend,
by substituting $a \oplus b$ into a :

The value which
we assign to b in
2. step.

$$a \equiv (a \oplus b) \oplus b$$

$$a \equiv a \oplus (b \oplus b)$$

(associative
property
of
XOR)

$$a \equiv a \oplus 0$$

$$a \equiv a$$

We just proved that
the value we assign to
 b in 2. step truly
is original a .