PROOF. (1) If $ab = ac$, we multiply by a^{-1} on the left and get $a^{-1}(ab) = a^{-1}(ac)$. Using associativity, -we obtain $(a^{-1}a)b = (a^{-1}a)c$. So $1b = lc$. Since 1 is the identity element of G, we finally get $b = c$.

(2) The proof of (2) is similar and is left to the reader. □

We must be careful when we want to use Lemma 8.1 to make cancel- lation. If the group is not commutative, left multiplication by an element and right multiplication by the same element give in general different results.In the proof of Lemma 8.l, we multiplied by a^{-1} on the same side. We cannot conclude $b = c$ from $ab = ca$, for instance. Indeed, we have

$ab = ca \Longrightarrow a^{-1}(ab) = a^{-1}(ac) \Longrightarrow (a^{-1}a)b = (a^{-1}c)a \Longrightarrow b = a^{-1}ca$

and this is all we can say.In general $a^{-1}ca \neq c$ so $b \neq c$.You must always ·make sure that you cancel on the same side.

Cancellations are multiplications by inverse elements. We now evaluate the inverse of an inverse, and the inverse of a product.

LEMMA 0.1. *Let G be a group and let $a, b \in G$. Then*
(1) $(a^{-1})^{-1} = a$,
(2) $(ab)^{-1} = b^{-1}a^{-1}$.

PROOF. (1) $aa^{-1} = l$ by the definition of a^{-1}.So a is a left inverse of a^{-1}.So a is the inverse of a^{-1}(Lemma 7.3).

(2) (ab)$(b^{-l}a^{-1})$ = a(b(b^{-l} a^{-1})) = a((b b^{-1}) a^{-1}) = a($1a^{-1}$) = a a^{-1} =1, and so b^{-l} a^{-1} is the inverse of a b. □

Therefore, the inverse of the inverse of an element is the element itself. Also, the inverse of a product is the product of the inverses, but in the reverse order. Do not write $(ab)^{-1} = a^{-1}b^{-1}$. This is wrong unless $a^{-1}b^{-1} = b^{-1}a^{-1}$, which is equivalent to $ab = ba$ (why?) and which is not true in general.