

```

theory Problem-1B
  imports HOL-Algebra.Algebra
begin

```

Problem 1B asks for a special case of Lagrange's theorem, thus we avoid using the general variant.

```

theorem (in comm-group) problem1B:
  assumes finite: finite (carrier G)
  assumes closed: g  $\in$  carrier G
  shows g [ $\wedge$ ] order G = 1
proof -
  let ?f =  $\lambda x. g \otimes x$ 
  have [simp]: ?f 'carrier G = carrier G
    by (simp add: closed group.surj-const-mult)
  have inj-on ?f (carrier G)
    by (simp add: closed group.inj-on-cmult)
  hence ( $\bigotimes x \in \text{carrier } G. x$ ) = ( $\bigotimes x \in \text{carrier } G. g \otimes x$ )
    using finprod-reindex[where h=?f and A=carrier G and f= $\lambda x. x$ , symmetric]
    by simp
  also have ... = ( $\bigotimes x \in \text{carrier } G. g$ )  $\otimes$  ( $\bigotimes x \in \text{carrier } G. x$ )
    using closed by (intro finprod-multf) auto
  finally have ( $\bigotimes x \in \text{carrier } G. g$ ) = 1
    using closed by (intro r-cancel-one'[THEN iffD1]) auto
  thus ?thesis
    using closed unfolding order-def by (simp add: finprod-const)
qed

end

```