

Theorem: Non-empty subuniverses (closed under the binary operation) of finite groups by the first definition (associative, cancellative and divisible) are subgroups.

Proof: Consider a subuniverse (S, \cdot) of finite (G, \cdot) .

Associativity: S has an associative operator, because G is a group and thus also has an associative operator.

Cancellative: Similarly S is cancellative, because G is a group:

$$\begin{aligned} \forall x, y, k \in G : k \cdot x = k \cdot y &\rightarrow x = y \\ \Rightarrow \\ \forall x, y, k \in S \subseteq G : k \cdot x = k \cdot y &\rightarrow x = y \end{aligned}$$

Divisibility:

We consider $x \in S, n = |S|$. If $x \cdot x \cdot x = x$, then x is a unit and is its own inverse.

We also consider $T = \{x, x^1, \dots, x^{n+1}\}$. From the pigeon principle it follows, that $\exists i, j : i < j : x^i = x^j$. This can be rewritten into: $x^i \cdot e = x^i \cdot x^{j-i}$. From the cancellative property $e = x^{j-i}$. Further, $x^{j-i-1} \in H$ (either $j - i > 1 \rightarrow x^{j-i-1} \in S$ or $j - i = 1 \rightarrow x^0 = e \in S$).

But $x \cdot x^{j-i-1} = x^{j-i} = e$, so for all $x \in S$ there exists an inverse and by extent (described in my previous homework) S is divisible.