Chapter 7.3 part 3

Th 7.16 Let F be a field.
Let G be a <u>finite</u> subgroup of F^*. $\Big\{ \prod_G e = 1_F$
Then G is cyclic.

Cor 7.10
Let G be a group. Let $c \in G$ be an element of G of the largest order.
Then for every $a \in G$ (of finite order), we have $|a| \mid |c|$ (not merely $|a| \leq |c|$)

Th 7.9 (1)
Let G be a group. Let $a \in G$, $|a| = n$.
$a^k = e$ if and only if $n \mid k$

Cor 4.17
Let F be a field. Let $f \in F[x]$, $\deg f = n$.
Then f has at most n roots

If $a \in F$ is a root, then
$f = (x-a)h$ $\deg f = \deg h + 1$
$h \in F[x]$

Pf (of Th 7.16)

Since G is finite, every its element has a finite order, and there are finitely many elements. Thus there is an element, call it $c \in G$ of the maximum order. Goal: $G = \langle c \rangle$. Obviously, $\langle c \rangle \subseteq G$

Let $|c| = m$ (the maximum order for an element of G)

By Cor 7.10, for every $a \in G$, $|a| \mid m$.

Thus, by Th 7.9(1), $a^m = e = 1_F$

That is: every $a \in G \subset F^*$ is a root of the polynomial

$x^m - 1_F \in F[x]$ $\qquad$ $\deg(x^m - 1_F) = m$

Cor 4.17 allows us to conclude that

$$|G| \leq m$$

At the same time, $|\langle c \rangle| = |c|$ (by Th 7.15)

$|\langle c \rangle| = m$ $\qquad$ $\langle c \rangle \subseteq G$ $\qquad$ $|G| \leq m$

We thus conclude that $\langle c \rangle = G$ (the subset $\langle c \rangle$ exhausts G)

G is cyclic