Proof. If these fields have p^m elements, by the above corollary they are both splitting fields of the polynomial $x^{p^m} - x$, over J_p whence they are isomorphic.

Thus for any integer m and any prime number p there is, up to isomorphism, at most one field having p^m elements. The purpose of the next lemma is to demonstrate that for any prime number p and any integer m there is a field having p^m elements. When this is done we shall know that there is exactly one field having p^m elements where p is an arbitrary prime and m an arbitrary integer.

LEMMA 7.1.4 *For every prime number p and every positive integer m there exists a field having p^m elements.*

Proof. Consider the polynomial $x^{p^m} - x$ in $J_p[x]$, the ring of polynomials in x over J_p, the field of integers mod p. Let K be the splitting field of this polynomial. In K let $F = \{a \in K \mid a^{p^m} = a\}$. The elements of F are thus the roots of $x^{p^m} - x$, which by Corollary 2 to Lemma 5.5.2 are distinct; whence F has p^m elements. We now claim that F is a field. If $a, b \in F$ then $a^{p^m} = a$, $b^{p^m} = b$ and so $(ab)^{p^m} = a^{p^m}b^{p^m} = ab$; thus $ab \in F$. Also since the characteristic is p, $(a \pm b)^{p^m} = a^{p^m} \pm b^{p^m} = a \pm b$, hence $a \pm b \in F$. Consequently F is a subfield of K and so is a field. Having exhibited the field F having p^m elements we have proved Lemma 7.1.4.

Combining Lemmas 7.1.3 and 7.1.4 we have

THEOREM 7.1.1 *For every prime number p and every positive integer m there is a unique field having p^m elements.*

We now return to group theory for a moment. The group-theoretic result we seek will determine the structure of any finite multiplicative subgroup of the group of nonzero elements of any field, and, in particular, it will determine the multiplicative structure of any finite field.

[illegible]

LEMMA 7.1.5 *Let G be a finite abelian group enjoying the property that the relation $x^n = e$ is satisfied by at most n elements of G, for every integer n. Then G is a cyclic group.*

Proof. If the order of G is a power of some prime number q then the result is very easy. For suppose that $a \in G$ is an element whose order is as large as possible; its order must be q^r for some integer r. The elements $e, a, a^2, \ldots, a^{q^r - 1}$ give us q^r distinct solutions of the equation $x^{q^r} = e$, which, by our hypothesis, implies that these are all the solutions of this equation. Now if $b \in G$ its order is q^s where $s \leq r$, hence $b^{q^r} = (b^{q^s})^{q^{r-s}} = e$. By the observation made above this forces $b = a^i$ for some i, and so G is cyclic.

The general finite abelian group G can be realized as $G = S_{q_1}S_{q_2}, \ldots, S_{q_k}$ where the q_i are the distinct prime divisors of $o(G)$ and where the S_{q_i} are the Sylow subgroups of G. Moreover, every element $g \in G$ can be written in a *unique* way as $g = s_1s_2, \ldots, s_k$ where $s_i \in S_{q_i}$ (see Section 2.7). Any solution of $x^n = e$ in S_{q_i} is one of $x^n = e$ in G so that each S_{q_i} inherits the hypothesis we have imposed on G. By the remarks of the first paragraph of the proof, each S_{q_i} is a cyclic group; let a_i be a generator of S_{q_i}. We claim that $c = a_1a_2, \ldots, a_k$ is a cyclic generator of G. To verify this all we must do is prove that $o(G)$ divides m, the order of c. Since $c^m = e$, we have that $a_1{}^m a_2{}^m \cdots a_k{}^m = e$. By the uniqueness of representation of an element of G as a product of elements in the S_{q_i}, we conclude that each $a_i{}^m = e$. Thus $o(S_{q_i}) \mid m$ for every i. Thus $o(G) = o(S_{q_1})o(S_{q_2}) \cdots o(S_{q_k}) \mid m$. However, $m \mid o(G)$ and so $o(G) = m$. This proves that G is cyclic.

Lemma 7.1.5 has as an important consequence

LEMMA 7.1.6 *Let K be a field and let G be a finite subgroup of the multiplicative group of nonzero elements of K. Then G is a cyclic group.*

Proof. Since K is a field, any polynomial of degree n in $K[x]$ has at most n roots in K. Thus in particular, for any integer n, the polynomial $x^n - 1$ has at most n roots in K, and all the more so, at most n roots in G. The hypothesis of Lemma 7.1.5 is satisfied, so G is cyclic.

Even though the situation of a finite field is merely a special case of Lemma 7.1.6, it is of such widespread interest that we single it out as

THEOREM 7.1.2 *The multiplicative group of nonzero elements of a finite field is cyclic.*

Proof. Let F be a finite field. By merely applying Lemma 7.1.6 with $F = K$ and $G =$ the group of nonzero elements of F, the result drops out.

We conclude this section by using a counting argument to prove the existence of solutions of certain equations in a finite field. We shall need the result in one proof of the Wedderburn theorem.

LEMMA 7.1.7 *If F is a finite field and $\alpha \neq 0$, $\beta \neq 0$ are two elements of F then we can find elements a and b in F such that $1 + \alpha a^2 + \beta b^2 = 0$.*

Proof. If the characteristic of F is 2, F has 2^n elements and every element x in F satisfies $x^{2^n} = x$. Thus every element in F is a square. In particular $\alpha^{-1} = a^2$ for some $a \in F$. Using this a and $b = 0$, we have