Let $K$ be a field and $f(x)$ be a nonconstant polynomial of $K[x]$. Then $f(x)$ is called irreducible in $K[x]$ if every factorization $f(x) = a(x)b(x)$ in $K[x]$ has $\{\deg a, \deg b\} = \{0, \deg f\}$. (This corresponds to prime numbers in $\mathbb{Z}$.) Otherwise $f(x)$ is reducible.

We begin with an important, general result. (It is Theorem A.2.22 of the Algebra Appendix.)

(A.2.22) Let $f(x) \in K[x]$ for $K$ a field, with $\deg f \geq 1$. Then the ring $K[x] \pmod{f(x)}$ is a field if and only if $f(x)$ is irreducible.

**Proof.** Assume that $f(x)$ is irreducible. Everything needed for $K[x] \pmod{f(x)}$ to be a field is clear except for the claim that all nonzero elements have multiplicative inverses.

Suppose that $g(x)$ is not zero in $K[x] \pmod{f(x)}$. That is, suppose that $g(x)$ is not a multiple of $f(x)$. Then $\gcd(g(x), f(x)) = \gcd(r(x), f(x))$, where $r(x)$ is the remainder upon division of $g(x)$ by $f(x)$. The polynomial $r(x)$ has degree less than $\deg f$ and is nonzero since $g(x)$ is not a multiple of $f(x)$.

Thus $\gcd(g(x), f(x)) = \gcd(r(x), f(x))$ is a divisor of $f(x)$ that has degree less than $f(x)$. As $f(x)$ is irreducible, that degree must be 0. Therefore monic $\gcd(g(x), f(x)) = \gcd(r(x), f(x)) = 1$. Now by the Extended Euclidean Algorithm, there are $s(x)$ and $t(x)$ in $K[x]$ with $s(x)g(x) + t(x)f(x) = 1$. That is, $s(x)g(x) = 1 \pmod{f(x)}$, and $s(x)$ is an inverse for $g(x)$ in the field $K[x] \pmod{f(x)}$.

Conversely suppose that $f(x)$ is reducible, and let $f(x) = a(x)b(x)$ be a factorization with $0 < \deg a < \deg f$ and $0 < \deg b < \deg f$. Then in the ring $K[x] \pmod{f(x)}$ the elements $a(x)$ and $b(x)$ are nonzero but have zero product. The ring is therefore not a field. \(\square\)

From now on, $F$ will denote a finite field.

(1) $F$ contains a copy of $\mathbb{Z}_p = \mathbb{F}_p$, for some prime $p$. (This prime is called the characteristic of $F$.)

**Proof.** Consider the apparently infinite subset

\[
\{1, 1+1, 1+1+1, \ldots \}
\]

of the finite field $F$. \(\square\)

(2) There is a positive integer $d$ with $|F| = p^d$.

**Proof.** From the definitions, $F$ is a vector space over $\mathbb{F}_p$. Let $e_1, \ldots, e_d$ be a basis. Then $F = \{\sum_{i=1}^{d} a_i e_i \mid a_1, \ldots, a_d \in \mathbb{F}_p\}$. Thus $|F|$ is the number of choices for the $a_i$, namely $p^d$. \(\square\)

(3) Let $\alpha \in F \geq \mathbb{F}_p$, and let $m(x) \in \mathbb{F}_p[x]$ be a monic polynomial of minimal degree with $m(\alpha) = 0$. (It exists since $F$ is finite.) Then $m(x)$ is irreducible and

\[
\mathbb{F}_p[\alpha] = \left\{ \sum_{i=0}^{k} a_i \alpha^i \mid k \geq 0, \ a_i \in \mathbb{F}_p \right\}
\]

is a subfield of $F$ that is a copy of $\mathbb{F}_p[x] \pmod{m(x)}$.

**Proof.** It is clear that the arithmetic of $\mathbb{F}_p[\alpha]$ is the same as that of $\mathbb{F}_p[x] \pmod{m(x)}$.

Suppose that $m(x)$ is reducible, and let $m(x) = a(x)b(x)$ be a factorization with $0 < \deg a < \deg m$ and $0 < \deg b < \deg m$. Then $a(\alpha)b(\alpha) = m(\alpha) = 0$. Therefore either $a(\alpha) = 0$ or $b(\alpha) = 0$. But both contradict our choice of $m(x)$ as a nonzero polynomial of minimal degree having $\alpha$ as a root. So $m(x)$ is not reducible and is irreducible. In particular, by Theorem A.2.22, $\mathbb{F}_p[\alpha]$ is a field. \(\square\)
The polynomial \( m(x) \) is called the **minimal polynomial** of \( \alpha \) over \( \mathbb{F}_p \) and is uniquely determined. We sometimes write \( m_\alpha(x) \) or even \( m_{\alpha, \mathbb{F}_p}(x) \) for the minimal polynomial of \( \alpha \) over \( \mathbb{F}_p \).

\[ F = \{0\} \cup \{1, \alpha, \alpha^2, \ldots, \alpha^i, \ldots, \alpha^{q-2}\}. \]

**Proof.** (sketch)

(i) For every \( \beta \) in \( F \setminus \{0\} \), the smallest positive \( h \) with \( \beta^h = 1 \) is a divisor of \( q - 1 \). (Consider the equivalence relation on \( F \setminus \{0\} \) given by \( \alpha \sim \omega \) if and only if \( \alpha \omega^{-1} \) is a power of \( \beta \).

(ii) For every \( h \) that divides \( q - 1 \) there are at most \( h \) elements \( \beta \) of \( F \setminus \{0\} \) with \( \beta^h = 1 \) by Proposition A.2.10.

(iii) By counting, we see that the total number of elements of \( F \setminus \{0\} \) that satisfy \( \beta^h = 1 \) for any \( h \) smaller than \( q - 1 \) is itself less than \( q - 1 \). Therefore there is at least one \( \alpha \) with \( 1, \alpha, \alpha^2, \ldots, \alpha^{q-2} \) all distinct and \( \alpha^{q-1} = 1 \). \( \Box \)

An element \( \alpha \) with \( F = \{0\} \cup \{1, \alpha, \alpha^2, \ldots, \alpha^i, \ldots, \alpha^{q-2}\} \) is called a **primitive element** in \( F \), and its minimal polynomial \( m_\alpha(x) \) is a **primitive polynomial**.

**Proof.** (sketch)

(i) For every \( \beta \) in \( F \setminus \{0\} \), the smallest positive \( h \) with \( \beta^h = 1 \) is a divisor of \( q - 1 \). (Consider the equivalence relation on \( F \setminus \{0\} \) given by \( \alpha \sim \omega \) if and only if \( \alpha \omega^{-1} \) is a power of \( \beta \).

(ii) For every \( h \) that divides \( q - 1 \) there are at most \( h \) elements \( \beta \) of \( F \setminus \{0\} \) with \( \beta^h = 1 \) by Proposition A.2.10.

(iii) By counting, we see that the total number of elements of \( F \setminus \{0\} \) that satisfy \( \beta^h = 1 \) for any \( h \) smaller than \( q - 1 \) is itself less than \( q - 1 \). Therefore there is at least one \( \alpha \) with \( 1, \alpha, \alpha^2, \ldots, \alpha^{q-2} \) all distinct and \( \alpha^{q-1} = 1 \). \( \Box \)

An element \( \alpha \) with \( F = \{0\} \cup \{1, \alpha, \alpha^2, \ldots, \alpha^i, \ldots, \alpha^{q-2}\} \) is called a **primitive element** in \( F \), and its minimal polynomial \( m_\alpha(x) \) is a **primitive polynomial**.

**Proof.** (sketch)

(i) For every \( \beta \) in \( F \setminus \{0\} \), the smallest positive \( h \) with \( \beta^h = 1 \) is a divisor of \( q - 1 \). (Consider the equivalence relation on \( F \setminus \{0\} \) given by \( \alpha \sim \omega \) if and only if \( \alpha \omega^{-1} \) is a power of \( \beta \).

(ii) For every \( h \) that divides \( q - 1 \) there are at most \( h \) elements \( \beta \) of \( F \setminus \{0\} \) with \( \beta^h = 1 \) by Proposition A.2.10.

(iii) By counting, we see that the total number of elements of \( F \setminus \{0\} \) that satisfy \( \beta^h = 1 \) for any \( h \) smaller than \( q - 1 \) is itself less than \( q - 1 \). Therefore there is at least one \( \alpha \) with \( 1, \alpha, \alpha^2, \ldots, \alpha^{q-2} \) all distinct and \( \alpha^{q-1} = 1 \). \( \Box \)

An element \( \alpha \) with \( F = \{0\} \cup \{1, \alpha, \alpha^2, \ldots, \alpha^i, \ldots, \alpha^{q-2}\} \) is called a **primitive element** in \( F \), and its minimal polynomial \( m_\alpha(x) \) is a **primitive polynomial**.

**Proof.** (sketch)

(i) For every \( \beta \) in \( F \setminus \{0\} \), the smallest positive \( h \) with \( \beta^h = 1 \) is a divisor of \( q - 1 \). (Consider the equivalence relation on \( F \setminus \{0\} \) given by \( \alpha \sim \omega \) if and only if \( \alpha \omega^{-1} \) is a power of \( \beta \).

(ii) For every \( h \) that divides \( q - 1 \) there are at most \( h \) elements \( \beta \) of \( F \setminus \{0\} \) with \( \beta^h = 1 \) by Proposition A.2.10.

(iii) By counting, we see that the total number of elements of \( F \setminus \{0\} \) that satisfy \( \beta^h = 1 \) for any \( h \) smaller than \( q - 1 \) is itself less than \( q - 1 \). Therefore there is at least one \( \alpha \) with \( 1, \alpha, \alpha^2, \ldots, \alpha^{q-2} \) all distinct and \( \alpha^{q-1} = 1 \). \( \Box \)

An element \( \alpha \) with \( F = \{0\} \cup \{1, \alpha, \alpha^2, \ldots, \alpha^i, \ldots, \alpha^{q-2}\} \) is called a **primitive element** in \( F \), and its minimal polynomial \( m_\alpha(x) \) is a **primitive polynomial**.

**Proof.** (sketch)

(i) For every \( \beta \) in \( F \setminus \{0\} \), the smallest positive \( h \) with \( \beta^h = 1 \) is a divisor of \( q - 1 \). (Consider the equivalence relation on \( F \setminus \{0\} \) given by \( \alpha \sim \omega \) if and only if \( \alpha \omega^{-1} \) is a power of \( \beta \).

(ii) For every \( h \) that divides \( q - 1 \) there are at most \( h \) elements \( \beta \) of \( F \setminus \{0\} \) with \( \beta^h = 1 \) by Proposition A.2.10.

(iii) By counting, we see that the total number of elements of \( F \setminus \{0\} \) that satisfy \( \beta^h = 1 \) for any \( h \) smaller than \( q - 1 \) is itself less than \( q - 1 \). Therefore there is at least one \( \alpha \) with \( 1, \alpha, \alpha^2, \ldots, \alpha^{q-2} \) all distinct and \( \alpha^{q-1} = 1 \). \( \Box \)

An element \( \alpha \) with \( F = \{0\} \cup \{1, \alpha, \alpha^2, \ldots, \alpha^i, \ldots, \alpha^{q-2}\} \) is called a **primitive element** in \( F \), and its minimal polynomial \( m_\alpha(x) \) is a **primitive polynomial**.