Teorema 1. *Sia k un campo finito. Allora $\#k$ è una potenza di un numero primo.*

Dimostrazione. Poiché k è finito, il suo sottocampo primo non può essere $\mathbf{Q}$ ed è quindi uguale a $\mathbf{Z}_p$ per un certo numero primo p . Come conseguenza k diventa uno spazio vettoriale su $\mathbf{Z}_p$ di dimensione n per un certo intero $n \geq 1$. Il campo k ha quindi p^n elementi come richiesto.

Teorema 2. *Sia k un campo di q elementi. Allora*

- (a) *si ha che $x^q = x$ per ogni $x \in k$;*
- (b) *Il gruppo k^* è ciclico di ordine $q - 1$.*

Dimostrazione. (a) Poiché $\#k^* = q - 1$, il Teorema di Lagrange implica che $x^{q-1} = 1$ per ogni $x \in k^*$. Come conseguenza si ha che $x^q = x$ per ogni $x \in k$.

(b) Ogni sottogruppo finito del gruppo moltiplicativo di un dominio è ciclico. In particolare il gruppo k^* è ciclico.

Teorema 3. *Per ogni potenza q di un numero primo p esiste un campo finito di cardinalità q . Il campo $\mathbf{F}_q$ è unico a meno di isomorfismi.*

Dimostrazione. Sia q una potenza di p . Sia $\overline{\mathbf{Z}}_p$ una chiusura algebrica di $\mathbf{Z}_p$. L'insieme

$$F = \{x \in \overline{\mathbf{Z}}_p : x^q = x\}$$

è un sottocampo di $\overline{\mathbf{Z}}_p$. Il polinomio $X^q - X \in \mathbf{Z}_p[X]$ non ha zeri doppi, perché la sua derivata è uguale a $qX^{q-1} - 1 = -1$ e non ha zeri. La cardinalità di F è quindi uguale al grado q del polinomio $X^q - X$. Questo dimostra che F è un campo di q elementi.

Per vedere l'unicità, sia k un campo di q elementi. Ogni chiusura algebrica C di k è anche una chiusura algebrica di $\mathbf{Z}_p$ ed è quindi isomorfa al campo $\overline{\mathbf{Z}}_p$. Il suo sottocampo $F = \{x \in C : x^q = x\}$ ha quindi q elementi. Per il Teorema 2 si ha che $x^q = x$ per ogni $x \in k$. Questo implica che $k \subset F$. Poiché $\#k = \#F = q$, si ha che $k = F$. Questo dimostra che tutti i campi di cardinalità q sono isomorfi.

Notazione. La notazione per l'unico campo di q elementi è $\mathbf{F}_q$. In particolare si ha che $\mathbf{F}_p = \mathbf{Z}_p$.

Per un numero primo p e per un polinomio irriducibile $f \in \mathbf{Z}_p[X]$ di grado d l'anello $\mathbf{Z}_p[X]/(f)$ è un campo finito di cardinalità $q = p^d$.

Esempio 1. L'unico polinomio irriducibile di grado 2 in $\mathbf{Z}_2[X]$ è $X^2 + X + 1$. Il campo $\mathbf{F}_4 = \mathbf{Z}_2[X]/(X^2 + X + 1)$ è l'insieme $\{0, 1, \alpha, \alpha + 1\}$ dove α è uno zero del polinomio $X^2 + X + 1$. Notiamo che $\alpha^2 = \alpha + 1$.

Teorema 4. *Sia p un primo e siano K e K' due sottocampi di $\overline{\mathbf{F}}_p$. Sia $\#K = p^n$ e $\#K' = p^{n'}$. Allora si ha che $K \subset K'$ se e solo se n divide n' . In particolare, per ogni $n \geq 1$ il campo $\overline{\mathbf{F}}_p$ contiene un unico sottocampo di cardinalità p^n .*

Dimostrazione. Se $K \subset K'$, allora K' è uno K -spazio vettoriale e quindi $\#K'$ è una potenza di $\#K$. Questo implica che n divide n' . Per dimostrare il viceversa osserviamo

che il Teorema 2 ci dice che $K = \{x \in \overline{\mathbf{F}}_p : x^{p^n} = x\}$ mentre $K' = \{x \in \overline{\mathbf{F}}_p : x^{p^{n'}} = x\}$. Se $x^{p^n} = x$ per un $x \in \overline{\mathbf{F}}_p$, allora $x^{p^{en}} = x$ per ogni intero $e \geq 1$. Se n divide n' , si ha quindi che $x^{p^{n'}} = x$. In altre parole, K è contenuto in K' come richiesto.

Teorema 5. *Sia p un primo, sia $q = p^n$ e sia $\alpha \in \mathbf{F}_q$. Allora il grado del polinomio minimo di α su $\mathbf{Z}_p$ divide n .*

Dimostrazione. Sia $f \in \mathbf{Z}_p[X]$ il polinomio minimo di α su $\mathbf{Z}_p$. Sia $d = \deg f$. Abbiamo che $\mathbf{Z}_p(\alpha) \subset \mathbf{F}_q$. Poiché $\mathbf{Z}_p(\alpha) = \mathbf{Z}_p[\alpha] \cong \mathbf{Z}_p[X]/(f)$ ha grado d su $\mathbf{Z}_p$, il Teorema 4 implica che d divide n come richiesto.

Teorema 6. *Sia p un primo, sia $n \geq 1$ e sia $q = p^n$. Allora*

(a) *esiste un polinomio irriducibile $f \in \mathbf{Z}_p[X]$ di grado n ;*

(b) *esiste $\alpha \in \overline{\mathbf{F}}_p$ tale che $\mathbf{F}_q = \mathbf{Z}_p(\alpha)$.*

Dimostrazione. Sia α un generatore del gruppo ciclico $\mathbf{F}_q^*$. Allora si ha che $\mathbf{Z}_p(\alpha) = \mathbf{F}_q$ e quindi il grado del polinomio minimo di α è uguale a n . Questo dimostra il teorema.

Teorema 7. *Sia p un primo e sia $q = p^n$ una potenza di p . Allora si ha che*

$$\prod_{\substack{f \in \mathbf{F}_p[X] \text{ irr.} \\ \deg f | n}} f(X) = X^q - X.$$

Dimostrazione. Sia $x \in \overline{\mathbf{F}}_p$ zero di un polinomio irriducibile f di grado un divisore di n . Per il Teorema 4 si ha che $\mathbf{F}_p(\alpha) \subset \mathbf{F}_q$ e quindi $x^q = x$. Viceversa, se $x \in \overline{\mathbf{F}}_p$ è zero di $X^q - X$, allora x è elemento del sottocampo $\{x \in \overline{\mathbf{F}}_p : x^q = x\}$ di $q = p^n$ elementi. Per il Teorema 5 il grado del polinomio minimo di x divide n .

In conclusione, ogni zero del polinomio a sinistra è anche zero di $X^q - X$ e viceversa. Siccome i due polinomi non hanno zeri doppi, sono per forza uguali, come richiesto.

Teorema 8. *Sia p un primo e sia $f \in \mathbf{F}_p[X]$ un polinomio irriducibile di grado d . Sia $\alpha \in \overline{\mathbf{F}}_p[X]$ uno zero di f . Allora si ha che*

$$f(X) = \prod_{i=0}^{d-1} (X - \alpha^{p^i}).$$

Dimostrazione. Il campo $\mathbf{F}_p(\alpha)$ è un'estensione di grado d di $\mathbf{F}_p$. Quindi, d è la più piccola potenza ≥ 1 tale che $\alpha^{p^d} = \alpha$. Questo implica che gli elementi

$$\alpha, \alpha^p, \dots, \alpha^{p^{d-1}}$$

di $\mathbf{F}_p(\alpha)$ sono distinti fra loro.

Scriviamo $f = X^n + \dots + a_1 X + a_0 \in \mathbf{Z}_p[X]$. Abbiamo che

$$\begin{aligned} f(\alpha^p) &= \alpha^{pn} + \dots + a_1 \alpha^p + a_0, \\ &= (\alpha^n + \dots + a_1 \alpha + a_0)^p, \\ &= 0. \end{aligned}$$

E quindi anche α^p è zero di f . Ripetendo quest'argomento vediamo che $\alpha, \alpha^p, \dots, \alpha^{p^{d-1}}$ sono d zeri di f . Poiché sono distinti fra loro, concludiamo che

$$f(X) = \prod_{i=0}^{d-1} (X - \alpha^{p^i}),$$

come richiesto.

Teorema 9. *Sia p un primo e sia $q = p^n$ una potenza di p . Allora*

- (a) *la mappa 'di Frobenius' φ data da $x \mapsto x^p$ è un automorfismo di $\mathbf{F}_q$;*
- (b) *Il gruppo $\text{Aut } \mathbf{F}_q$ degli automorfismi di $\mathbf{F}_q$ è il gruppo ciclico di ordine n generato da φ .*

Dimostrazione. (a) La mappa di Frobenius φ è un omomorfismo di campi. Poiché $\mathbf{F}_q$ è finito, il fatto che φ è iniettiva implica che è suriettiva. Osserviamo che il fatto che n è la più piccola potenza tale che $x^{p^n} = x$ per ogni $x \in \mathbf{F}_q$ implica che l'ordine dell'automorfismo di Frobenius è uguale a n .

(b) Sia ψ un automorfismo di $\mathbf{F}_q$. Per il Teorema 6 (b) si ha che $\mathbf{F}_q = \mathbf{F}_p(\alpha)$ per un certo elemento α . Sia $f = X^n + \dots a_1 X + a_0 \in \mathbf{F}_p[X]$ il polinomio minimo di α . Poiché ψ fissa il sottocampo primo $\mathbf{F}_p$, si ha che

$$\begin{aligned} f(\psi(\alpha)) &= \psi(\alpha)^n + \dots a_1 \psi(\alpha) + a_0, \\ &= \psi(\alpha^n + \dots + a_1 \alpha + a_0), \\ &= 0. \end{aligned}$$

In altre parole, $\psi(\alpha)$ deve essere uno zero di f . Per il Teorema 8 si ha quindi che $\psi(\alpha) = \alpha^{p^i}$ per un certo $i = 0, 1, \dots, d-1$. Dal fatto che $\mathbf{F}_q = \mathbf{F}_p(\alpha)$ si deduce che $\psi(x) = x^{p^i}$ per ogni $x \in \mathbf{F}_q$. Poiché $x^{p^i} = \varphi^i(x)$, concludiamo che $\psi = \varphi^i$ come richiesto.

Teorema 10. *(Corrispondenza di Galois per $\mathbf{F}_q$) Sia p un primo e sia q una potenza di p . Sia $G = \text{Aut } \mathbf{F}_q$. Allora la mappa che ad un sottogruppo $H \subset G$ associa il sottocampo $\mathbf{F}_q^H = \{x \in \mathbf{F}_q : \sigma(x) = x \text{ per ogni } \sigma \in H\}$ è una biiezione*

$$\{\text{sottogruppi di } G\} \leftrightarrow \{\text{sottocampi di } \mathbf{F}_q\}.$$

Si ha che $[G : H] = \#\mathbf{F}_q^H$ per ogni sottogruppo $H \subset G$.

Dimostrazione. Scriviamo $q = p^n$. Il gruppo $G = \langle \varphi \rangle$ è ciclico di ordine n . Per ogni divisore d di n il sottogruppo $H = \langle \varphi^d \rangle$ è l'unico sottogruppo H di G di indice d . Similmente, il sottocampo di $\mathbf{F}_q$ fissato da H è uguale a $\{x \in \mathbf{F}_q : x^{p^d} = x\}$ e per il Teorema 4 esso è l'unico sottocampo di $\mathbf{F}_q$ di cardinalità p^d . Questo dimostra il teorema.

Tabella 1. Il campo $\mathbf{F}_{16}$.

α^i	additivo	polinomio minimo	ordine in $\mathbf{F}_{16}^*$
—	0	X	—
1	1	$X + 1$	1
α	α	$X^4 + X + 1$	15
α^2	α^2	$X^4 + X + 1$	15
α^3	α^3	$X^4 + X^3 + X^2 + X + 1$	5
α^4	$\alpha + 1$	$X^4 + X + 1$	15
α^5	$\alpha^2 + \alpha$	$X^2 + X + 1$	3
α^6	$\alpha^3 + \alpha^2$	$X^4 + X^3 + X^2 + X + 1$	5
α^7	$\alpha^3 + \alpha + 1$	$X^4 + X^3 + 1$	15
$\alpha^8 = \alpha^{-7}$	$\alpha^2 + 1$	$X^4 + X + 1$	15
$\alpha^9 = \alpha^{-6}$	$\alpha^3 + \alpha$	$X^4 + X^3 + X^2 + X + 1$	5
$\alpha^{10} = \alpha^{-5}$	$\alpha^2 + \alpha + 1$	$X^2 + X + 1$	3
$\alpha^{11} = \alpha^{-4}$	$\alpha^3 + \alpha^2 + \alpha$	$X^4 + X^3 + 1$	15
$\alpha^{12} = \alpha^{-3}$	$\alpha^3 + \alpha^2 + \alpha + 1$	$X^4 + X^3 + X^2 + X + 1$	5
$\alpha^{13} = \alpha^{-2}$	$\alpha^3 + \alpha^2 + 1$	$X^4 + X^3 + 1$	15
$\alpha^{14} = \alpha^{-1}$	$\alpha^3 + 1$	$X^4 + X^3 + 1$	15

Tabella 2. Il campo $\mathbf{F}_{27}$.

β^i	additivo	polinomio minimo	ordine in $\mathbf{F}_{27}^*$
—	0	X	—
1	1	$X - 1$	1
β	β	$X^3 - X + 1$	26
β^2	β^2	$X^3 + X^2 + X - 1$	13
β^3	$\beta - 1$	$X^3 - X + 1$	26
β^4	$\beta^2 - \beta$	$X^3 + X^2 - 1$	13
β^5	$-\beta^2 + \beta - 1$	$X^3 - X^2 + X + 1$	26
β^6	$\beta^2 + \beta + 1$	$X^3 + X^2 + X - 1$	13
$\beta^7 = -\beta^{-6}$	$\beta^2 - \beta - 1$	$X^3 + X^2 - X + 1$	26
$\beta^8 = -\beta^{-5}$	$-\beta^2 - 1$	$X^3 - X^2 - X - 1$	13
$\beta^9 = -\beta^{-4}$	$\beta + 1$	$X^3 - X + 1$	26
$\beta^{10} = -\beta^{-3}$	$\beta^2 + \beta$	$X^3 + X^2 - 1$	13
$\beta^{11} = -\beta^{-2}$	$\beta^2 + \beta - 1$	$X^3 + X^2 - X + 1$	26
$\beta^{12} = -\beta^{-1}$	$\beta^2 - 1$	$X^3 + X^2 - 1$	13
$\beta^{13} = -1$	-1	$X + 1$	2
$\beta^{14} = -\beta$	$-\beta$	$X^3 - X - 1$	13
$\beta^{15} = -\beta^2$	$-\beta^2$	$X^3 - X^2 + X + 1$	26
$\beta^{16} = -\beta^3$	$-\beta + 1$	$X^3 - X - 1$	13
$\beta^{17} = -\beta^4$	$-\beta^2 + \beta$	$X^3 - X^2 + 1$	26
$\beta^{18} = -\beta^5$	$\beta^2 - \beta + 1$	$X^3 + X^2 + X - 1$	13
$\beta^{19} = -\beta^6$	$-\beta^2 - \beta - 1$	$X^3 - X^2 + X + 1$	26
$\beta^{20} = \beta^{-6}$	$-\beta^2 + \beta + 1$	$X^3 - X^2 - X - 1$	13
$\beta^{21} = \beta^{-5}$	$\beta^2 + 1$	$X^3 + X^2 - X + 1$	26
$\beta^{22} = \beta^{-4}$	$-\beta - 1$	$X^3 - X - 1$	13
$\beta^{23} = \beta^{-3}$	$-\beta^2 - \beta$	$X^3 - X^2 + 1$	26
$\beta^{24} = \beta^{-2}$	$-\beta^2 - \beta + 1$	$X^3 - X^2 - X - 1$	13
$\beta^{25} = \beta^{-1}$	$-\beta^2 + 1$	$X^3 - X^2 + 1$	26

NB. Poiché $X^3 - X + 1 = (X - \beta)(X - \beta^3)(X - \beta^9)$, si ha che $\beta^{13} = \beta\beta^3\beta^9 = -1$.