Corso di Crittografia A.A. 2017-2018

Note sui campi finiti

Leonardo Tamiano

November 6, 2018

Contents

1 Caratteristica di un campo

Sia $(\mathbb{K}, +, \cdot)$ un campo. Notiamo che $\mathbb{K}$ è anche un anello commutativo e unitario, ovvero esiste l'elemento neutro $1 \in \mathbb{K}$ per la seconda operazione. Possiamo dunque considerare la seguente applicazione $\varphi : \mathbb{Z} \to \mathbb{K}$ che mappa l'anello degli interi $\mathbb{Z}$ nel campo $\mathbb{K}$ e definita da:

- $\varphi(0) = 0$
- $\forall n \in \mathbb{Z}^+ : \varphi(n) = \underbrace{1 + 1 + ... + 1}_{\text{n volte}}$
- $\forall n \in \mathbb{Z}^- : \varphi(-n) = -\varphi(n)$

Notiamo che tale applicazione è un *omomorfismo tra anelli* in quanto sono rispettate le seguenti condizioni

1. $\varphi(n + m) = \varphi(n) + \varphi(n)$
2. $\varphi(n \cdot m) = \varphi(n) \cdot \varphi(m)$

Ora, se l'applicazione φ risulta essere iniettiva, allora diciamo che il campo $\mathbb{K}$ ha **caratteristica 0**. In questo caso possiamo sommare 1 con se stesso un numero arbitrario di volte in $\mathbb{K}$ senza mai ottenere lo 0. Di campi a caratteristica 0 ce ne sono molti, ad esempio $\mathbb{R}$ è un campo a caratteristica 0. In generale si vede che un campo a caratteristica 0 è necessariamente infinito in quanto "contiene" interamente $\mathbb{Z}$. Il viceversa non è vero in quanto esistono campi infiniti che non hanno caratteristica 0.

Nel caso in cui l'applicazione φ non è iniettiva, ovvero se $\mathbb{K}$ non è un campo a caratteristica 0, allora diciamo che $\mathbb{K}$ è un campo a **caratteristica** n, dove n è l'intero positivo più piccolo tale che sommando 1 a se stesso n volte in $\mathbb{K}$ otteniamo lo 0. Un fatto notevole è il seguente: se questo n esiste, allora è primo. Supponiamo infatti che non lo sia e consideriamo una sua fattorizzazione non banale $n = ab$. Abbiamo

$$\varphi(n) = \varphi(a)\varphi(b) = 0$$

ma $\mathbb{K}$ è un campo, e quindi è anche un *dominio di integrità*, ovvero è un anello commutativo e unitario in cui il prodotto di elementi non nulli è sempre un elemento non nullo, o, in formula, tale che

$$\forall a, b \in \mathbb{K} : a \cdot b = 0 \implies [a = 0 \vee b = 0]$$

Quindi abbiamo $\varphi(a) = 0$ o $\varphi(b) = 0$. Notiamo infine che questo non può succedere in quanto avevamo definito n come il più piccolo intero positivo tale che $\varphi(n) = 0$. Quindi se un campo non ha caratteristica 0 allora ha caratteristica p, per qualche primo $p \in \mathbb{Z}$.

1.1 Sottoanello fondamentale di un campo $\mathbb{K}$

Sia $\mathbb{K}$ un campo e sia φ l'applicazione definita prima che mappa l'anello degli interi $\mathbb{Z}$ nel campo $\mathbb{K}$. Notiamo (senza dimostrare) che il *nucleo* di φ, definito come

$$Ker(\varphi) = \{n \in \mathbb{Z} : \varphi(n) = 0\} \subset \mathbb{Z}$$

è un *ideale* di $\mathbb{Z}$. Dato che $\mathbb{Z}$ è a *ideali principali*, sappiamo che esiste un $n \in \mathbb{Z}$ tale che $Ker(\varphi) = (n)$. Per campi $\mathbb{K}$ a caratteristica 0 l'ideale $Ker(\varphi)$ è l'ideale nullo generato da 0, mentre per campi $\mathbb{K}$ a caratteristica p, l'ideale $Ker(\varphi)$ è l'ideale generato da (p).

Se un campo $\mathbb{K}$ ha caratteristica 0 allora tale campo contiene una copia isomorfica di $\mathbb{Z}$. Possiamo infatti mettere in biiezione $\varphi(\mathbb{Z})$, intesa come l'immagine di φ, e $\mathbb{Z}$ ottenendo un *isomorfismo*. Per questa ragione diciamo che $\mathbb{Z}$ è il *sottoanello fondamentale* di $\mathbb{K}$ quando $\mathbb{K}$ è un campo a caratteristica 0.

Invece, se il campo $\mathbb{K}$ ha caratteristica p, con p primo, allora non è più $\mathbb{Z}$ ad essere "contenuto" (sempre a livello di isomorfismo) in $\mathbb{K}$. In questo caso troviamo una copia isomorfica di $\mathbb{Z}_p$ all'interno di $\mathbb{K}$. Questo fatto segue da un teorema dell'algebra astratta noto come *teorema fondamentale di omomorfismo*, che essenzialmente dice che se $f : A \to B$ è un omomorfismo di anelli, allora, posto $Ker(f)$ come il nucleo di f e $Img(f)$ come l'immagine di f, troviamo il seguente isomorfismo

$$A/Ker(f) \simeq Img(f)$$

Senza perdere troppo tempo sul pensare all'oggetto $A/Ker(f)$ (è l'anello quoziente di A modulo $Ker(f)$), applicando il teorema al nostro caso particolare poniamo $A = \mathbb{Z}$, $Ker(\varphi) = (p)$, e conoscendo che $\mathbb{Z}/(p) = \mathbb{Z}_p$ (la costruzione formale di $\mathbb{Z}_p$ è proprio $\mathbb{Z}/(p)$), otteniamo

$$\mathbb{Z}/(p) = \mathbb{Z}_p \simeq Img(\varphi) \subset \mathbb{K}$$

Per questa ragione si dice che l'anello fondamentale di $\mathbb{K}$ è $\mathbb{Z}_p$ quando $\mathbb{K}$ è un campo a caratteristica p.

Dato che noi lavoreremo principalmente con campi finiti, questi campi avranno necessariamente una caratteristica diversa da 0, e quindi posto $\mathbb{F}$ un campo finito e posta p la caratteristica di $\mathbb{F}$, sappiamo che $\mathbb{F}$ contiene una copia isomorfica di $\mathbb{Z}_p$.

2 Ordine di un campo finito

Sia $\mathbb{F}$ un campo finito. Dalla discussione precedente sappiamo che $\mathbb{F}$ ha caratteristica p, con p primo. Andiamo adesso a studiare l'ordine di $\mathbb{F}$, ovvero il numero di elementi di $\mathbb{F}$. A tal fine utilizzeremo nozioni prese dall'algebra lineare.

Ricordiamo che dato un campo generale $\mathbb{F}$ possiamo definire sul campo $\mathbb{F}$ uno

spazio vettoriale V, ovvero un insieme i cui elementi sono chiamati *vettori* e che rispettano varie proprietà che non riportiamo per brevità.

Dato che $\mathbb{F}$ ha caratteristica p, sappiamo che $\mathbb{F}$ contiene un sottoinsieme isomorfo a $\mathbb{Z}_p$, o, per dirla in modo meno formale, che $\mathbb{Z}_p \subset \mathbb{F}$. Ma p è primo, e quindi $\mathbb{Z}_p$ è un campo. Possiamo dunque considerare $\mathbb{F}$ come spazio vettoriale su $\mathbb{Z}_p$. Notiamo che questa è una scelta sensata in quanto è possibile dimostrare che $\mathbb{F}$ rispetta tutte le proprietà per poter essere considerato uno spazio vettoriale sul campo $\mathbb{Z}_p$. Dato che $\mathbb{F}$ è finito, anche la dimensione di $\mathbb{F}$ come spazio vettoriale su $\mathbb{Z}_p$ deve essere finita . Sia f tale dimensione e sia $\{v_1, v_2, ..., v_f\}$ una base di $\mathbb{F}$ come spazio vettoriale su $\mathbb{Z}_p$. Dato che ogni elemento di $\mathbb{F}$ si scrive in modo unico come

$$a_1 v_1 + a_2 v_2 + ... + a_f v_f$$

con gli $a_i \in \mathbb{Z}_p$, e dato che ogni a_i può assumere esattamente p valori, concludiamo che $\mathbb{F}$ ha p^f elementi.

Generalmente con $\mathbb{F}_q$ si indica un campo finito di ordine q. Da quanto visto in questa sezione sappiamo quindi che $q = p^f$, con p primo e $f \in \mathbb{N}^+$.

3 $\mathbb{F}_q^*$ è un gruppo ciclico

Sia $\mathbb{F}_q$ un campo finito con $q = p^f$, p primo. Lo scopo di questa sezione è analizzare il gruppo formato dall'insieme $\mathbb{F}_q^* := \mathbb{F}_q \setminus \{0\}$ e dalla seconda operazione di $\mathbb{F}_q$ (la "moltiplicazione"). In particolare dimostreremo che $\mathbb{F}_q^*$ è un *gruppo ciclico*, ovvero che esiste un $g \in \mathbb{F}_q^*$ tale che le sue potenze ci permettono di ottenere ogni elemento di $\mathbb{F}_q^*$. Simbolicamente,

$$\mathbb{F}_q^* = \{g^i : i \in \mathbb{N}\} =: \langle g \rangle$$

Ricordiamo brevemente che per *ordine di un elemento a di un gruppo G* intendiamo il più piccolo intero positivo t tale che $a^t = 1$ in G. Indichiamo con $ord_G(a)$ l'ordine di a nel gruppo G; se poi il gruppo G è intuibile dal contesto possiamo scrivere anche solamente $ord(a)$.

Per mostrare che $\mathbb{F}_q^*$ è un gruppo ciclico dobbiamo dimostrare che esiste sempre un elemento di $\mathbb{F}_q^*$ il cui ordine è $q-1$. Infatti, se $a \in \mathbb{F}_q^*$ con $ord(a) = q-1$ allora le potenze di a generano $q-1$ elementi distinti, che sono proprio tutti gli elementi di $\mathbb{F}_q^*$ (il fatto che gli elementi della forma a^i sono distinti per $0 < i < q-1$ segue dal fatto che $ord(a) = q-1$).

Lo schema che seguiremo per ottenere questo risultato è più o meno il seguente

1. Dimostriamo che l'ordine di ogni elemento di $\mathbb{F}_q^*$ divide $q-1$.
2. Caratterizziamo in un modo particolare gli elementi di ordine d in $\mathbb{F}_q^*$.

3. Utilizzando una identità conosciuta dimostriamo che ci sono $\varphi(d)$ elementi di ordine d in $\mathbb{F}_q^*$, dove $\varphi : \mathbb{N} \to \mathbb{N}$ è la funzione di eulero definita da $\varphi(0) = 0$ e

$$\forall n \in \mathbb{N}^+ : \varphi(n) := \{m \in \mathbb{N} : 0 < m < n, MCD(n, m) = 1\}$$

In particolare questo implichera che ci sono $\varphi(q-1) > 0$ elementi di ordine $q-1$ in $\mathbb{F}_q^*$, e quindi che $\mathbb{F}_q^*$ è ciclico.

3.1 Parte 1: $a \in \mathbb{F}_q^* \implies ord(a) \mid q-1$.

Lemma 3.1. Sia a un elemento del gruppo $\mathbb{F}_q^*$. Allora $ord(a) \mid q-1$.

Proof. Sia a un elemento di $\mathbb{F}_q^*$. L'idea della dimostrazione è di rappresentare gli elementi di $\mathbb{F}_q^*$ come prodotti della forma ax, con $x \in \mathbb{F}_q^*$. Notiamo che questa diversa rappresentazione ci ritorna tutti gli elementi di $\mathbb{F}_q^*$ senza ripetizioni. Infatti, se abbiamo $ax = ay$ dividendo per a otteniamo $x = y$. Inoltre, posto $x \in \mathbb{F}_q^*$, ho che $a^{-1}x \in \mathbb{F}_q^*$ e quindi $a(a^{-1}x) = x$. Ma allora moltiplicando tutti gli elementi di $\mathbb{F}_q^*$ in queste diverse rappresentazioni otteniamo lo stesso elemento di $\mathbb{F}_q^*$,

$$\prod_{x \in \mathbb{F}_q^*} x = \prod_{x \in \mathbb{F}_q^*} ax = a^{q-1} \prod_{x \in \mathbb{F}_q^*} x \iff a^{q-1} = 1$$

Osserviamo infine che questo implica che $ord(a) | q-1$. Infatti, se per assurdo non fosse così, ovvero se $ord(a) \not| q-1$, allora posto $e = MCD(ord(a), q-1)$ abbiamo che esistono $A, B \in \mathbb{Z}$ tali che

$$ord(a)A + (q-1)B = e$$

e quindi

$$a^e = a^{ord(a)A+(q-1)B} = (a^{ord(a)})^A (a^{q-1})^B = 1 \cdot 1 = 1$$

ma $ord(a)$ non divide $q-1$, e quindi $e = MCD(ord(a), q-1) < ord(a)$, il che è un assurdo in quanto $a^e = 1$. □

3.2 Parte 2

Proposizione 3.1. Sia a un elemento del gruppo $\mathbb{F}_q^*$ e supponiamo che a ha ordine d in $\mathbb{F}_q^*$. Allora l'insieme degli elementi di ordine d in $\mathbb{F}_q^*$ è dato da

$$\{a^i : 0 < i < q-1 : MCD(i, d) = 1\}$$

che sono esattamente $\varphi(d)$.

Proof. Consideriamo il polinomio

$$f(x) = x^d - 1 \in \mathbb{F}_q[X]$$

Notiamo che a è una radice di tale polinomio in quanto a ha ordine d e quindi $a^d = 1$, ovvero $a^d - 1 = 0$ in $\mathbb{F}_q$. In realtà questo non vale solo per a ma vale per tutti gli elementi generati da a. Più precisamente, per ogni $i = 0, ..., d-1$ abbiamo che a^i è una radice di tale polinomio in quanto

$$(a^i)^d - 1 = (a^d)^i - 1 = 1^i - 1 = 0$$

Abbiamo quindi trovato d radici di tale polinomio. Notiamo poi che $\mathbb{F}_q$ è un campo, e un risultato noto è che un polinomio f di grado n a coefficienti in un campo può avere al più n radici, ciascuna considerata con la sua molteplicità. Nel nostro caso abbiamo che $f(x)$ è un polinomio di grado d a coeffienti nel campo $\mathbb{F}_q$ e quindi può avere solamente d radici, considerate con la loro molteplicità. Queste d radici sono proprio gli elementi generati da a. Concludiamo affermando che tutte e sole le radici di $f(x)$ sono contenute in $\{1, a, ..., a^{d-1}\}$.

Ora, dato che ogni elemento di ordine d è sicuramente una radice di $f(x)$, possiamo inferire per quanto visto prima che gli elementi di ordine d, essendo radici di $f(x)$, sono contenuti in $\langle a \rangle = \{1, a, ..., a^{d-1}\}$.

Dimostriamo adesso che gli elementi di ordine d sono le potenze a^i tali che $MCD(i, d) = 1$. Questo segue dalle seguenti due osservazioni:

1. Sia a^i una potenza di a tale che $MCD(i, d) = e > 1$, allora

   $$(a^i)^{d/e} = (a^d)^{i/e} = 1$$

   e quindi $ord(a^i) \leq d/e < d$. In questo caso a^i non può avere ordine d.

2. Sia a^i una potenza di a tale che $MCD(i, d) = 1$ e supponiamo per assurdo che $d' = ord(a^i) < d$. Allora, utilizzando il fatto che esistono A, B tali che $iA + dB = 1$ troviamo

   $$\begin{aligned} a^{d'} = (a^{d'})^1 &= (a^{d'})^{iA+dB} \\ &= (a^i)^{d'A} \cdot (a^d)^{d'B} = 1 \end{aligned}$$

   Infatti valgono le seguenti

   - $(a^i)^{d'A} = ((a^i)^{d'})^A = 1^A = 1$
   - $(a^d)^{d'B} = 1^{d'B} = 1$

   Ma questo è un assurdo in quanto $d' < d$ e l'ordine di a era proprio d. Concludiamo che $d' \geq d$.

   Notiamo però che $d' \leq d$ per il semplice fatto che

   $$(a^i)^d = (a^d)^i = 1^i = 1$$

   Ma allora in questo casto a^i ha ordine d.

□

3.3 Parte 3

Ricapitolando, abbiamo appena finito di dimostrare che se a è un elemento di $\mathbb{F}_q^*$ di ordine d, allora gli elementi di ordine d sono le potenze a^i tali che $MCD(i,d) = 1$. Notiamo però che questo non basta per dimostrare che $\mathbb{F}_q^*$ è ciclico in quanto non sappiamo se esiste un elemento di ordine $q-1$ in $\mathbb{F}_q^*$. Procediamo quindi con l'ultimo passo.

Teorema 3.1. Gli elementi di ordine d in $\mathbb{F}_q^*$ sono esattamente $\varphi(d)$, e, se a è un elemento di ordine d, allora a^i è un'altro elemento di ordine d se e solo se $MCD(i,d) = 1$.

Proof. Per dimostrare questo teorema utilizzeremo la seguente identità, dimostrata nella lezione 4 del 21 marzo 2018:

$$\forall n \in \mathbb{N} : \sum_{d|n} \varphi(d) = n$$

Per iniziare definiamo per ogni $d \mid q-1$,

$$\sigma(d) := \text{numero di elementi di } \mathbb{F}_q^* \text{ che hanno ordine } d$$

Notiamo che da quanto visto prima si ha che se $\sigma(d) > 0$, allora $\sigma(d) = \varphi(d)$. Otteniamo quindi,

$$\forall d \mid q-1 : \sigma(d) \leq \varphi(d)$$

Notiamo poi che è possibile partizionare $\mathbb{F}_q^*$ in base all'ordine dei vari elementi, ovvero

$$\mathbb{F}_q^* = \bigcup_{d|q-1} \{a \in \mathbb{F}_q^* : ord(a) = d\}$$

tale partizionamento, unità all'identità di φ mostrata prima, ci permette di ottenere la seguente relazione

$$[q-1 = \sum_{d|q-1} \sigma(d) \leq \sum_{d|q-1} \varphi(d) = q-1] \implies \sum_{d|q-1} \sigma(d) = \sum_{d|q-1} \varphi(d)$$

Ci basta poi osservare che l'unico caso in cui tale relazione è verificata è quando $\forall d \mid q-1 : \sigma(d) = \varphi(d)$. Infatti, supponiamo per assurdo che non sia così, ovvero supponiamo che esiste un d^* tale che $\sigma(d^*) \neq \varphi(d^*)$. Allora $\sigma(d^*) = 0$ e quindi

$$\sum_{d|q-1} \sigma(d) < \sum_{d|q-1} \varphi(d)$$

in quanto per tutti i d diversi da d^* si ha che $\sigma(d) \leq \varphi(d)$ e per d^* si ha $\sigma(d^*) < \varphi(d^*)$.

Abbiamo quindi dimostrato che il numero di elementi di $\mathbb{F}_q^*$ che hanno ordine d è $\varphi(d)$. Per l'ultima parte invece basta vedere la dimostrazione della proposizione precedente. □

Osservazione 3.1. Notiamo che anche se sappiamo che il gruppo $\mathbb{F}_q^*$ associato al campo finito $\mathbb{F}_q$ è un gruppo ciciclo, trovare un generatore di tale gruppo rimane comunque un problema difficile. Non a caso la dimostrazione fornita è una dimostrazione non-costruttiva.

4 Chi sono gli elementi di $\mathbb{F}_q$?

Presentiamo adesso una caratterizzazione degli elementi di $\mathbb{F}_q$ che utilizza il concetto di polinomio. Campi finiti e polinomi sono infatti strettamente legati e, come elaboreremo successivamente, i polinomi tra le altre cose ci forniscono un modo piuttosto naturale di estendere i campi finiti.

Teorema 4.1. Gli elementi di $\mathbb{F}_q$ sono tutte e sole le radici del polinomio

$$f(x) = x^q - x \in \mathbb{F}_q[X]$$

Proof. Sia $a \in \mathbb{F}_q$. Se $a = 0$ allora a è radice di $f(x)$; altrimenti $a \in \mathbb{F}_q^*$ e, per quanto visto prima, si ha

$$a^{q-1} = 1 \iff a^q = a \iff a^q - a = 0$$

ovvero a è radice di $f(x)$.

Notiamo infine che $f(x)$ non può avere più di q radici, contante con la loro molteplicità, in quanto è un polinomio i cui coefficienti risiedono nel campo $\mathbb{F}_q$. Infine, $f(x)$ non ha radici doppie in quanto la derivata di $f(x)$ è $f'(x) = qx^{q-1} - 1 = p^f x^{q-1} - 1 = -1$ e una proposizione ci dice che una eventuale radice doppia di f dovrebbe essere anche una radice di f'. □

5 Estensioni di campi

Sia E un campo e sia F un sottoinsieme di E. Se anche F è un campo, allora diciamo che F è un *sottocampo* di E o, equivalentemente, che il campo E è una *estensione* del campo F. Noi siamo interessati a studiare queste estensioni per due ragioni: come prima cosa ci permetteranno di risolvere qualsiasi polinomio su qualsiasi campo. Infatti, se $f(x)$ è un polinomio a coefficienti in un campo F può succedere che non tutte le radici di $f(x)$ sono contenute in F. Si dimostra però che *esiste sempre* una particolare estensione di F che contiene *tutte* le radici di $f(x)$. Studiare estensioni di campi ci aiuterà poi per la costruzione del campo finito $\mathbb{F}_q$, con $q = p^f$. Si vedrà infatti che tale campo è una particolare estensione del campo finito $\mathbb{Z}_p$.

5.1 Utilizzare i polinomi per estendere un campo

Ricordiamo che se F è un campo allora indichiamo con $F[X]$ l'anello dei polinomi a coefficenti nel campo F. $F[X]$ sarà quindi composto da espressioni della forma

$$a_0 + a_1 x^1 + ... + a_n x^n$$

con gli $a_i \in F$. Noi siamo interessati ai polinomi a coefficienti in F perché ci permettono di rappresentare le varie estensioni di F. Segue una breve discussione teorica su come è possibile utilizzare i polinomi per estendere un campo F.

Sia E un campo, F un sottocampo di E e sia $c \in E$. Definiamo la *funzione di sostituzione* $\sigma_c : F[X] \to E$ come segue,

$$\forall f(x) \in F[X] : \sigma_c(f(x)) := f(c) \in E$$

Quindi σ_c è la funzione "sostituisci x per c". Notiamo che questa funzione è un *omomorfismo* in quanto valgono le seguenti

- $\sigma_c(f(x)g(x)) = f(c)g(c) = \sigma_c(f(x))\sigma_c(g(x))$
- $\sigma_c(f(x) + g(x)) = f(c) + g(c) = \sigma_c(f(x)) + \sigma_c(g(x))$

Consideriamo ora il kernel di σ_c. Notiamo che tale kernel è formato da tutti i polinomi $f(x) \in F[x]$ tali che $f(c) = 0$, ovvero è formato da tutti i polinomi $f(x) \in F[X]$ tali che c è una radice di $f(x)$. Denotiamo con J_c tale kernel. Dato che J_c è il kernel di un omomorfismo, è possibile dimostrare che J_c è un ideale di $F[X]$.

Assumiamo che c è la radice di qualche polinomio in $F[X]$, ovvero che J_c non è l'ideale nullo. In questo caso diciamo che c è *algebrico su* F. Se c non è algebrico su F, ovvero se c non è la radice di nessun polinomio di $F[X]$, allora diciamo che c è *trascendente su* F e si ha $J_c = (0)$. Dato che il caso trascendente non ci permette di costruire una estensione di F, questo caso particolare viene escluso.

Ricordiamo che $F[X]$ è a ideali principale, in particolare quindi l'ideale J_c è generato da un singolo polinomio in $F[X]$. Sia $p(x)$ tale polinomio, ovvero sia $p(x)$ tale che $J_c = \langle p(x) \rangle$. Facciamo le seguenti osservazioni sul polinomio $p(x)$:

- Dato che $p(x)$ deve generare J_c, il grado di $p(x)$ deve necessariamente essere *il più piccolo* tra tutti i polinomi non nulli in J_c.
- Notiamo inoltre che $p(x)$ è necessariamente *irriducibile in* $F[X]$. Infatti, supponendo per assurdo che $p(x)$ è riducibile in $F[X]$, troviamo due polinomi non costanti $f(x), g(x) \in F[X]$ tali che $p(x) = f(x)g(x)$. Ma allora $p(c) = f(c)g(c) = 0$, e dato che $F[X]$ è un dominio di integrità abbiamo che $f(c) = 0$ oppure $g(c) = 0$. In entrambi i casi troviamo un polinomio di grado più piccolo del grado di $p(x)$ che si trova nell'ideale generato da $p(x)$, il che è un assurdo.
- Notiamo che J_c contiene anche tutti i multipli *costanti* di $p(x)$. Possiamo dunque imporre senza perdità di generalità che $p(x)$ è un polinomio *monico*, ovvero che il coefficiente del termine di grado massimo di $p(x)$ è 1. Allora $p(x)$ è l'unico polinomio monico irriducibile di grado più piccolo in J_c. Questo polinomio prende il nome di *polinomio minimo* di c su F.

Abbiamo appena finito di analizzare il kernel di σ_c. Occupiamoci ora del range di σ_c, denotato da $Img(\sigma_c)$. Notiamo che dato che σ_c è un omomorfismo, allora $Img(\sigma_c)$ è chiuso rispetto all'addizione, alla moltiplicazione, e ai negativi (inversi rispetto all'addizione). Notiamo infine che il range di σ_c è anche chiuso rispetto alla moltiplicazione. Sia infatti $f(c) \in Img(\sigma_c)$ non nullo, allora sappiamo che $f(x)$ non fa parte dell'idale generato da $p(x)$. Dato che $p(x)$ è irriducibile ne consegue che $f(x)$ e $p(x)$ non hanno fattori in comune, e quindi $MCD(f(x), p(x)) = 1$. Ma allora possiamo trovare una *identità di Bézout* tra $f(x)$ e $p(x)$, ovvero esistono dei polinomi $s(x)$ e $t(x)$ tali che $s(x)f(x) + t(x)p(x) = 1$. Ma allora,

$$s(c)f(c) + t(c)p(c) = 1$$

e dato che $p(c) = 0$ troviamo che $s(c)f(c) = 1$ in $Img(\sigma_c)$, ovvero $s(c)$ è l'inverso moltiplicativo di $f(c)$.

Abbiamo quindi dimostrato che $Img(\sigma_c)$ è un campo, e in particolare è un sottocampo di E. Notiamo ora che

$$Img(\sigma_c) = \{f(c) : f(x) \in F[X]\}$$

ovvero il range di σ_c è formato da tutti e soli gli elementi della forma

$$a_0 + a_1 c + ... + a_n c^n$$

con gli $a_i \in F$ e $n \in \mathbb{N}$. In altre parole, il range di σ_c è il *più piccolo campo che contiene F e c*. Tale campo viene chiamato il campo *generato da F e c* e viene indicato con il simbolo molto importante

$$F(c)$$

La terminologia "il più piccolo campo che contiene F e c" significa che $F(c)$ contiene F e c e $F(c)$ è contenuto da ogni altro campo che contiene F e c.

Terminando, osserviamo che abbiamo un omomorfismo σ_c con dominio $F[X]$, range $F(c)$ e il cui kernel è $J_c = \langle p(x) \rangle$. Dal *teorema fondamentale di omomorfismo* otteniamo che

$$F(c) \simeq F[X]/\langle p(x) \rangle$$

5.1.1 Ok, ma quindi come faccio a estendere un campo?

La discussione presentata prima potrebbe essere un pochino pesante e fare riferimento a risultati teorici non studiati. In ogni caso l'idea di come procedere per estendere un campo F risiede tutta nel seguente isomorfismo

$$F(c) \simeq F[X]/\langle p(x) \rangle$$

Il nostro obiettivo adesso sarà capire come utilizzare questo strano isomorfimo per estendere un campo F.

Iniziamo descrivendo brevemente l'insieme $F[X]/\langle p(x)\rangle$. Tale insieme è formato da classi di equivalenza modulo $p(x)$. In altre parole, se $p(x)$ è un polinomio di grado d, allora

$$F[X]/\langle p(x) = \{a_0 + a_1x + ... + a_{d-1}x^{d-1} : a_i \in F\}$$

Inoltre le operazioni di somma e prodotto nell'insieme vengono effettuate modulo $p(x)$, il che vuol dire che dati due polinomi $f(x), g(x) \in F[X]/\langle p(x)\rangle$ per sapere chi è il polinomio $f(x)+g(x)$ in $F[X]/\langle p(x)\rangle$, ci basta fare la somma dei polinomi $f(x) + g(x)$ e prendere il resto nella divisione per $p(x)$ (divisione tra polinomi). La stessa cosa vale per quanto riguarda la moltiplicazione.

Sia F un campo e supponiamo di voler estendere F. Come possiamo procedere? Il problema è che trovare delle estensioni di un campo F è molto diverso dal trovare dei sottocampi di F. Per trovare un sottocampo di F gli elementi da analizzare sono già noti, e il nostro compito si riduce semplicemente a pescare un insieme di elementi che formano un campo. Invece, se vogliamo trovare una estensione di F, dobbiamo in un senso molto reale *costruirla* partendo da F. Ovvero dobbiamo definire dei nuovi elementi, aggiungerli a F e ottenere un nuovo campo. Come costruiamo questi nuovi elementi?

Qui entrano in gioco, i polinomi. L'idea è quella di utilizzare le radici di polinomi irriducibili per estendere un campo. Più precisamente, sia $p(x)$ un polinomio irriducibile in $F[X]$. Se **definiamo** l'elemento c come la radice di $p(x)$, sappiamo che c sicuramente non sta in F. Dalla discussione precedente sappiamo poi che aggiungendo c ad F otteniamo il campo $F(c)$, e questo campo è isomorfo al campo $F[X]/\langle p(x)\rangle$. Ma quindi un possibile modo per estendere F è proprio l'insieme $F[X]/\langle p(x)\rangle$ con le operazioni di somma e prodotto di polinomi modulo $p(x)$.

Esempio 5.1. Un esempio molto famoso di estensione di campi è quello del passaggio dal campo dei reali $\mathbb{R}$ al campo dei complessi $\mathbb{C}$. Quando viene introdotto il campo dei complessi $\mathbb{C}$ si dice che è formato dalle coppie $a + ib$, con $a, b \in R$ e i tale che $i^2 = -1$. Le operazioni definite su $\mathbb{C}$ sono poi le seguenti

- $(a + ib) + (c + id) := (a + c) + i(b + d)$
- $(a + ib) \cdot (c + id) := (ac - bd) + i(ad + bc)$

Proviamo ora a dare senso a tale definizione. Come sappiamo, per estendere un campo si utilizzano le radici di polinomi irriducibili. Nel caso di $\mathbb{R}$ si può dimostrare che i polinomi irriducibili sono i polinomi di primo grado e di secondo grado. Mentre le radici dei polinomi irriducibili di primo grado sono contenuti in $\mathbb{R}$, le radici dei polinomi irriducibili di scondo grado non lo sono. In particolare, un polinomio irriducibile di secondo grado in $\mathbb{R}$ è il polinomio

$$x^2 + 1 \in \mathbb{R}[X]$$

Abbiamo quindi trovato un polinomio irriducibile $p(x)$. Sia i una radice di tale polinomio, ovvero sia i un elemento tale che $i^2 + 1 = 0 \iff i^2 = -1$. Aggiungendo i a $\mathbb{R}$ otteniamo il campo $\mathbb{R}(i)$. Dalla discussione di prima sappiamo che $\mathbb{R}(i)$ è isomorfo al campo costituto dall'insieme

$$\mathbb{R}[X]/\langle x^2 + 1\rangle = \{a_0 + xa_1 : a_0, a_1 \in \mathbb{R}\}$$

e dalle solite operazioni di moltiplicazione e addizione tra polinomi modulo $x^2 + 1$.

La descrizione del campo $\mathbb{R}(i)$ che utilizza i polinomi potrebbe però essere vista, almeno le prime volte, come strana e non naturale. Se vogliamo ottenere la descrizione tradizionale di tale campo dobbiamo semplicemente utilizzare l'isomorfismo presente tra $\mathbb{R}[X]/\langle x^2 + 1\rangle$ e $\mathbb{R}(i)$. In particolare un isomorfismo è dato dalla funzione $f : \mathbb{R}[X]/\langle x^2 + 1\rangle \to \mathbb{R}(i)$ definita nel seguente modo

$$\forall a(x) \in \mathbb{R}[X]/\langle x^2 + 1\rangle : f(a(x)) = a(i)$$

Notiamo in particolare che il campo $\mathbb{R}(i)$ è formato dagli elementi

$$\mathbb{R}(i) = \{a + ib : a, b \in \mathbb{R}\}$$

e le operazioni sono ottenute utilizzando il fatto che i è la radice del polinomio $x^2 + 1$, ovvero che $i^2 = -1$. Abbiamo quindi ottenuto un campo con gli stessi elementi e con le stesse operazioni che avevamo definito per descrivere il campo dei complessi $\mathbb{C}$. In altre parole, il campo dei complessi $\mathbb{C}$ è proprio $\mathbb{R}(i)$,

$$\mathbb{C} = \mathbb{R}(i)$$

5.2 Estensioni di campi particolari

Se abbiamo un campo $\mathbb{K}$ possiamo pensare a estendere $\mathbb{K}$ per ottenere altri campi. Alcune di queste estensioni sono molto importanti all'interno della teoria dei campi. A seguire qualche esempio di estensione importante.

5.2.1 Campo di riducibilità completa

Sia $\mathbb{K}$ un campo e sia $f(x) \in \mathbb{K}[X]$. $\mathbb{K}'$ è detto campo di **riducibilità completa** di $f(x)$ se $\mathbb{K}'$ contiene tutte le radici di $f(x)$ ed è minimale sotto queste condizioni.

La terminologia campo di riducibilità completa di $f(x)$ significa intuitivamente che, dato che il campo $\mathbb{K}'$ contiene *tutte* le radici del polinomio $f(x)$, possiamo fattorizzare $f(x)$ in $\mathbb{K}'[X]$ nel seguente modo:

$$f(x) = c \cdot \prod_{i=1}^{h} (x - \alpha_i)^{m_i}$$

dove $c \in \mathbb{K}'$, $\alpha_1, ..., \alpha_h$ sono le radici di $f(x)$ e la radice $\alpha_i \in \mathbb{K}'$ ha molteplicità m_i.

Come faccio ad ottenere il campo di riducibilità completa partendo da un polinomio $f(x) \in \mathbb{K}[X]$? L'idea è semplice, poste $\alpha_1, ..., \alpha_n$ le radici di $f(x)$ quello che dobbiamo fare è calcolare il più piccolo campo che contiene sia $\mathbb{K}$ che tutte e n le radici $\alpha_1, \alpha_2, ..., \alpha_n$. Tale campo è rappresentato dal simbolo

$$\mathbb{K}(\alpha_1, \alpha_2, ..., \alpha_n)$$

Esempio 5.2. Sia $\mathbb{K} = \mathbb{R}$ e sia $f(x) = x^2 + 1 \in \mathbb{R}[X]$. Il campo di riducibilità completa di $f(x)$ è il campo ottenuto aggiungendo a $\mathbb{R}$ le radici di $f(x)$, che sono i e $-i$ con $i^2 = -1$. In questo caso aggiungendo i e $-i$ a $\mathbb{R}$ otteniamo il campo dei complessi $\mathbb{C}$. Possiamo dunque dire che $\mathbb{C}$ è il campo di riducibilità completa di $f(x)$.

Teorema 5.1. Il campo finito $\mathbb{F}_q$ è unico a meno di isomorfismi

Proof. Si può dimostrare che il campo di riducibilità completa di un polinomio è unico a meno di isomorfismi. Inoltre, posto $q = p^f$, si ha che $\mathbb{F}_q$ è il campo di riducibilità completa del polinomio $x^q - x \in \mathbb{Z}_p[X]$. □

Osservazione 5.1. Dal teorema segue che per ogni $f \in \mathbb{N}^+$ esiste un unico campo $\mathbb{F}_p^f$ a meno di isomorfismi.

5.2.2 Chiusura algebrica

Dato un campo $\mathbb{K}$, la **chiusura algebrica** di $\mathbb{K}$ è il campo $\bar{\mathbb{K}}$ definito come il più piccolo campo che contenga $\mathbb{K}$ e che sia **algebricamente chiuso**, ovvero che per ogni polinomio $f(x)$ non costante a coefficienti in $\mathbb{K}$ esiste almeno una radice di $f(x)$ in $\bar{\mathbb{K}}$.

Notiamo che anche se nella definizione di campo algebricamente chiuso chiediamo la presenza di almeno una radice per ogni polinomio non costante $f(x)$, questo in realtà implica che *ogni* polinomio a coefficienti in $\mathbb{K}$ ha *tutte* le radici nella chiusura algebrica di $\mathbb{K}$. Infatti, dato $f(x) \in \mathbb{K}[X]$ sappiamo che esiste una radice α di $f(x)$ nella chiusura algebrica di $\mathbb{K}$. Possiamo poi dividere $f(x)$ per $x - \alpha$ per ottenere un nuovo polinomio, sempre a coefficienti in $\mathbb{K}$, che ha una nuova radice β nella chiusura algebrica di $\mathbb{K}$. Iterando questo ragionamento vediamo come la chiusura algebrica di $\mathbb{K}$ contiene *tutte* le radici di *tutti* i polinomi a coefficienti in $\mathbb{K}$.

Anche la chiusura algebrica di un campo è unica a meno di isomorfismi.

Esempio 5.3. Sia $\mathbb{K} = \mathbb{R}$. Per ottenere la chiusura algebrica di $\mathbb{R}$ dobbiamo analizzare tutti i polinomi irriducibili in $\mathbb{R}$ e verificare quali sono i polinomi irriducibili le cui radici non si trovano in $\mathbb{R}$. Si può dimostrare che in $\mathbb{R}$ gli unici polinomi irriducibili sono quelli di primo e secondo grado. In particolare la radici di polinomi irriducibili non contenute in $\mathbb{R}$ sono i e $-i$ con $i^2 = -1$. Andando ad aggiungere queste radici ad $\mathbb{R}$ otteniamo il campo dei complessi $\mathbb{C}$, che risulta essere proprio la chiusura algebrica di $\mathbb{R}$.

5.3 Estensioni di $\mathbb{Z}_p$

Sia $\mathbb{F}_q$ un campo finito. Sappiamo che $q = p^f$ con p primo e sappiamo che $\mathbb{F}_q$ contiene al suo interno una copia isomorfica di $\mathbb{Z}_p$. Dato che $\mathbb{F}_q$ è ottenuto da $\mathbb{Z}_p$ aggiungendo determinati elementi, diciamo che $\mathbb{F}_q$ è una *estensione* di $\mathbb{Z}_p$. In particolare quindi ogni campo finito $\mathbb{F}_q$ sarà l'estensione di un campo della forma $\mathbb{Z}_p$ con p primo.

Sia $\xi \in \mathbb{F}_q$ e consideriamo $\mathbb{Z}_p(\xi)$, ovvero il più piccolo campo contenente $\mathbb{Z}_p$ e ξ. Notiamo che anche $\mathbb{Z}_p(\xi)$ è una estensione di $\mathbb{Z}_p$. Dato che $\mathbb{Z}_p(\xi)$ stesso è un campo finito abbiamo che $\mathbb{Z}_p(\xi) = \mathbb{F}_{p^d}$ per qualche $d \in \mathbb{N}$. Abbiamo quindi la seguente relazione

$$\mathbb{Z}_p \subseteq \mathbb{Z}_p(\xi) = \mathbb{F}_{p^d} \subseteq \mathbb{F}_{p^f}$$

Andiamo adesso a studiare la relazione tra d e f.

Notiamo che $\mathbb{Z}_p(\xi) = \mathbb{F}_{p^d}$ è uno spazio vettoriale su $\mathbb{Z}_p$ di dimensione d. Anche $\mathbb{F}_{p^f}$ è uno spazio vettoriale su $\mathbb{Z}_p(\xi)$. Sia δ la dimensione di $\mathbb{F}_p^f$ come spazio vettoriale su $\mathbb{Z}_p(\xi)$. Abbiamo quindi le seguenti relazioni

$$\begin{cases} \mathbb{F}_{p^f} \simeq (\mathbb{F}_{p^d})^\delta \\ \mathbb{F}_{p^d} \simeq (\mathbb{Z}_p)^d \end{cases} \implies \mathbb{F}_{p^f} \simeq (Z_p)^{d\delta}$$

ovvero il numero di elementi di $\mathbb{F}_q$ è $(p^d)^\delta$, e quindi $f = \delta \cdot d$, il che implica che $d \mid f$.

Osservazione 5.2. Abbiamo appena dimostrato che per avere una relazione del tipo $\mathbb{F}_{p^d} \subset \mathbb{F}_{p^f}$ dobbiamo avere $p \mid f$. Questo ad esempio ci permette di dire che $\mathbb{F}_8$ non contiene $\mathbb{F}_4$ per il semplice fatto che $4 = 2^2$, $8 = 2^3$ e $2 \not| 3$.

Se aggiungendo ξ a $\mathbb{Z}_p$ otteniamo il campo $\mathbb{Z}_p(\xi) = \mathbb{F}_{p^d}$ allora diciamo che $\mathbb{Z}_p(\xi)$ è una *estensione di grado d*, o equivalentemente che ξ *ha grado d*. In particolare ξ ha grado d se ξ è la radice di un polinomio irriducibile in $\mathbb{Z}_p[X]$ di grado d.

5.4 Costruzione del campo finito $\mathbb{F}_{p^f}$

Supponiamo di voler costruire il campo $\mathbb{F}_{p^f}$. Possiamo dividere il processo di costruzione di $\mathbb{F}_{p^f}$ nei seguenti passi:

1. Si vede che $\mathbb{F}_{p^f}$ è una estensione di grado f di $\mathbb{Z}_p$.
2. Si cominciano a enumerare tutti i polinomi monici in $\mathbb{Z}_p[X]$ di grado f. Tra questi poi si selezionano quelli irriducibili, scartando quelli riducibili.
3. Sia $p(x)$ uno dei polinomi selezionati nel passo 2). Qual'è esattamente il polinomio selezionato non importa per la costruzione, la cosa importante è che tale polinomio sia un polinomio monico irriducibile di grado f a coefficienti in $\mathbb{Z}_p$.

4. Utilizzando risultati visti precedentemente il campo finito $\mathbb{F}_{p^f}$ è isomorfo al campo $\mathbb{Z}_p[X]/\langle p(x)\rangle$. Un primo modo per descriverlo è quindi il seguente

$$\mathbb{Z}_p[X]/\langle p(x)\rangle = \{a_0 + a_1x + ... + a_{f-1}x^{f-1} : a_0, a_1, ..., a_{f-1} \in \mathbb{Z}_p\}$$

   Notiamo infatti che tale insieme ha esattamente p^f elementi, come ci aspettavamo. Per quanto riguarda le operazioni sappiamo che le operazioni di somma e prodotto tra polinomi vengono eseguiti modulo $p(x)$.

5. Un modo alternativo di descrivere il campo finito $\mathbb{F}_{p^f}$ è di definire un elemento α come la radice del polinomio $p(x)$. A questo punto l'insieme sarà formato dai seguenti elementi

$$\mathbb{F}_{p^f} = \{a_0 + a_1\alpha + ... + a_{f-1}\alpha^{f-1} \ : a_0, a_1, ..., a_{f-1} \in \mathbb{Z}_p\}$$

   e le tabelle di somma e prodotto vengono definite utilizzando il fatto che $\mathbb{F}_{p^f}$ è un campo a caratteristica p e che $p(\alpha) = 0$.

5.4.1 Costruzione di $\mathbb{F}_4$

Come prima cosa notiamo che $\mathbb{F}_4$ è una estensione di grado 2 di $\mathbb{Z}_2$. Andando poi a enumerare i polinomi monici di grado 2 a coefficienti in $\mathbb{Z}_2$ troviamo la seguente situazione

Polinomio monico di grado 2 in $\mathbb{Z}_2[X]$	è irriducibile in $\mathbb{Z}_2[X]$?
x^2	No
$x^2 + 1$	No
$x^2 + x$	No
$x^2 + x + 1$	Si

Nel nostro caso quindi il polinomio irrudicibile è solo uno ed è $p(x) = x^2 + x + 1$. Ma allora otteniamo

$$\mathbb{F}_4 \simeq \mathbb{Z}_2[X]/\langle x^2 + x + 1\rangle = \{0, 1, x, x + 1\}$$

Le operazioni in tale insieme sono semplicemente somma e moltiplicazione tra i polinomi riducendo modulo $x^2 + x + 1$.

Infine, se vogliamo esprimere $\mathbb{F}_4$ utilizzando una radice di $p(x)$, sia α tale radice, ovverio sia α un elemento tale che $\alpha^2 = \alpha + 1$ (ricordiamo di lavorare in un campo a caratteristica 2, e quindi $1 = -1$). Otteniamo che gli elementi di $\mathbb{F}_4$ sono

$$\mathbb{F}_4 = \{0, 1, \alpha, \alpha + 1\}$$

Per quanto riguarda le tabelle di addizione e moltiplicazione, notiamo che la tabella di addizione è ottenuta utilizzando il fatto che $\mathbb{F}_4$ è un campo a caratteristica 2, e quindi che $2 = 0$ in $\mathbb{F}_4$. La tabella di moltiplicazione invece utilizza il fatto che α è la radice del polinomio x^2+x+1 e quindi che $\alpha^2 = \alpha+1$.

A seguire la tabella che descrive il modo in cui gli elementi si addizionano in $\mathbb{F}_4$.

$+$	0	1	α	$\alpha+1$
0	0	1	α	$\alpha+1$
1	1	0	$\alpha+1$	α
α	α	$\alpha+1$	0	1
$\alpha+1$	$\alpha+1$	α	1	0

A seguire la tabella che descrive il modo in cui gli elementi si moltiplicano in $\mathbb{F}_4$.

$\cdot$	0	1	α	$\alpha+1$
0	0	0	0	0
1	0	1	α	$\alpha+1$
α	0	α	$\alpha+1$	1
$\alpha+1$	0	$\alpha+1$	1	α

5.4.2 Costruzione di $\mathbb{F}_8$

Notiamo che $8 = 2^3$ e quindi $\mathbb{F}_8$ è una estensione di grado 3 di $\mathbb{Z}_2$. Nuovamente, andiamo a cercare un polinomio monico irriducibile di grado 3 in $\mathbb{Z}_2[X]$.

Polinomio monico di grado 3 in $\mathbb{Z}_2[X]$	è irriducibile in $\mathbb{Z}_2[X]$?
x^3	No
x^3+1	No
x^3+x	No
x^3+x^2	No
x^3+x+1	Si
x^3+x^2+1	Si
x^3+x^2+x	No
x^3+x^2+x+1	No

In questo caso abbiamo due polinomi irriducibili. Scegliamo il polinomio $p(x) = x^3+x+1$. Allora il campo finito $\mathbb{F}_8$ è isomorfo a

$$\mathbb{F}_8 \simeq \mathbb{Z}_2[X]/\langle x^3+x+1\rangle = \{0, 1, x, x+1, x^2, x^2+x, x^2+1, x^2+x+1\}$$

Come al solito le operazioni in $\mathbb{Z}_2[X]/\langle x^3+x+1\rangle$ vengono effettuate modulo x^3+x+1.

Per ottenere una diversa rappresentazione possiamo come al solito utilizzare le radici del polinomio $p(x)$. Sia α una radice di $p(x)$, ovvero sia α un elemento tale che $\alpha^3 = \alpha+1$. Allora l'insieme $\mathbb{F}_8$ sarà formato dagli elementi

$$\mathbb{F}_8 = \{0, 1, \alpha, \alpha+1, \alpha^2, \alpha^2+\alpha, \alpha^2+1, \alpha^2+\alpha+1\}$$

Infine, per ottenere le tabelle della moltiplicazione e addizione dobbiamo sempre utilizzare il fatto che $\mathbb{F}_8$ è un campo a caratteristica 2 e che $\alpha^3 = \alpha+1$.

5.4.3 Costruzione di $\mathbb{F}_9$

Notiamo che $9 = 3^2$. Dunque $\mathbb{F}_9$ è una estensione di grado 2 di $\mathbb{Z}_3$. Come al solito, andiamo a cercare un polinomio monico irriducibile di grado 2 in $\mathbb{Z}_3[X]$.

Polinomio monico di grado 2 in $\mathbb{Z}_3[X]$	è irriducibile in $\mathbb{Z}_3[X]$?
x^2	No
x^2+1	Si
x^2+2	No
x^2+x	No
x^2+2x	No
x^2+x+1	No
x^2+x+2	Si
x^2+2x+1	No
x^2+2x+2	Si

Questa volta ho tre polinomi monici irriducibili. Scegliamo tra questi $p(x) = x^2+1$. Il campo $\mathbb{F}_9$ è quindi isomorfo al campo

$$\begin{aligned}\mathbb{F}_9 \simeq \mathbb{Z}_3[X]/\langle x^2+1\rangle &= \{0,1,2,x,x+1,x+2,2x,2x+1,2x+2\}\\ &= \{0,1,-1,x,x+1,x-1,-x,-x+1,-x+-1\}\end{aligned}$$

le cui tabelle di addizione/moltiplicazione sono sempre modulo x^2+1.

Per quanto riguarda la seconda rappresentazione, ovvero la rappresentazione di $\mathbb{F}_9$ che utilizza le radici di $p(x)$ possiamo definire i tale che $i^2 = -1$ e descrivere $\mathbb{F}_9$ nel seguente modo

$$\mathbb{F}_9 = \{0,1,-1,i,i+1,-i,-i+1,-i-1\}$$

Nuovamente, le tabelle di addizione/moltiplicazione per questa rappresentazione sono ottenute utilizzando il fatto che lavoriamo in un campo a caratteristica 3, e quindi $3 = 0$, e che i è la radice del polinomio $p(x) = x^2+1$, ovvero $i^2 = -1$.

6 Automorfismo di Frobenius

Sia $q = p^f$ con p primo e consideriamo la seguente applicazione $\sigma : \mathbb{F}_q \to \mathbb{F}_q$, definita da

$$\forall x \in \mathbb{F}_q : \sigma(x) := x^p \in \mathbb{F}_q$$

Notiamo che σ è un *automorfismo*, infatti valgono le seguenti proprietà

1. $\sigma(xy) = (xy)^p = x^p y^p = \sigma(x)\sigma(y)$
2. $\sigma(x+y) = \sigma(x) + \sigma(y)$. Infatti

$$\begin{aligned}\sigma(x+y) = (x+y)^p &= \sum_{i=0}^{p} \binom{p}{i} x^{p-i} y^i\\ &= \binom{p}{0}x^p + \binom{p}{1}x^{p-1}y + ... + \binom{p}{p-1}xy^{p-1} + \binom{p}{p}y^p\\ &= x^p + y^p = \sigma(x) + \sigma(y)\end{aligned}$$

in quanto tutti i termini con $\binom{p}{i}, 0 < i < p$ sono multipli di p e quindi, dato che $\mathbb{F}_q$ è un campo a caratteristica p, sono tutti uguali a 0 in $\mathbb{F}_q$.

6.1 Punti fissi di σ

Notiamo che un punto $x \in \mathbb{F}_q$ è fissato da σ se e solo se $x^p = x$, ovvero se e solo se x è soluzione di $x^P - x$. Dato che $\mathbb{Z}_p$ è il campo di riducibilità completa di $x^p - x$ abbiamo che x è fissato da σ se e solo se $x \in \mathbb{Z}_p$.

Più generalmente abbiamo il seguente,

$$\begin{aligned} x \text{ è fissato da } \sigma^j &\iff x^{p^j} = x \\ &\iff x \text{ è soluzione di } x^{p^j} - x \\ &\iff x \in \mathbb{F}_{p^j} \end{aligned}$$

Quindi se consideriamo le potenze di σ troviamo che sono

$$\sigma, \sigma^2, ..., \sigma^f$$

e che σ^i fissa il sottocampo $\mathbb{F}_{p^i}$. In particolare $\sigma^f = id_{\mathbb{F}_q}$ in quanto σ^f fissa l'intero campo $\mathbb{F}_q$.

7 Come spezzare $x^{p^f} - x$ in $\mathbb{Z}_p[X]$

In questa sezione analizziamo come il polinomio $x^{p^f} - x$ può essere fattorizzato in $\mathbb{Z}_p[X]$. A tale fine vale il seguente

Teorema 7.1. In $\mathbb{Z}_p[X]$ il polinomio $x^{p^f} - x$ è il prodotto di tutti e soli i polinomi monici irriducibili di grado d con $d \mid f$.

Proof. Iniziamo dimostrando che $x^{p^f} - x$ è diviso da tutti i polinomi monici irriducibili di grado d con $d \mid f$. Sia $\Phi(x)$ un tale polinomio monico irriducibile di grado d con $d \mid f$ e sia α una radice di $\Phi(x)$.

Dato che $d \mid f$ ho la seguente situazione,

$$\mathbb{Z}_p \subseteq \mathbb{Z}_p(\alpha) = \mathbb{F}_{p^d} \subseteq F_{p^f}$$

quindi $\alpha \in \mathbb{F}_{p^f}$ e, in particolare, α è una radice di $x^{p^f} - x$. Ma allora il fattore $x - \alpha$ è condiviso tra $x^{p^f} - x$ e $\Phi(x)$. Possiamo quindi porre

$$MCD(\Phi(x), x^{p^f} - x) = \Psi(x)$$

ed essere sicuri che $\Psi(x)$ è almeno un polinomio di primo grado.

Notiamo però che $\Psi(x)$ è un polinomio a coefficienti in $\mathbb{Z}_p$. Infatti il calcolo del MCD tra due polinomi a coefficienti in $\mathbb{Z}_p$ mi da come risultato un altro polinomio a coefficienti in $\mathbb{Z}_p$. Inoltre $\Psi(x) \mid \Phi(x)$. Ma $\Psi(x)$ era stato assunto essere irriducibile in $\mathbb{Z}_p[X]$, e quindi otteniamo $\Psi(x) = \Phi(x) \mid x^{p^f} - x$.

Dimostriamo ora che ogni fattore di $x^{p^f} - x$ è un polinomio irriducibile in $\mathbb{Z}_p[X]$ di grado d con $d \mid f$. Sia $\Phi(x)$ un polinomio che divide $x^{p^f} - x$. Chiaramente $\Phi(x)$ è monico. Sia d il grado di $\Phi(x)$ e dimostriamo che $d \mid f$.

Notiamo che per ogni α radice di $\Phi(x)$ abbiamo che α è anche una radice di $x^{p^f} - x$. Ma quindi l'estensione ottenuta aggiungendo a $\mathbb{Z}_p$ una radice di $\Phi(x)$ è contenuta in $\mathbb{F}_{p^f}$, e questo implica che $d \mid f$. In formula, posta α una radice di $\Phi(x)$, si ha che

$$\mathbb{Z}_p \subseteq \mathbb{Z}_p(\alpha) = \mathbb{F}_{p^d} \subseteq \mathbb{F}_{p^f} \implies d \mid f$$

□

Corollario 7.1. Siano p, f numeri primi. Allora esistono

$$\frac{p^f - p}{f}$$

polinomi monici irriducibili di grado f in $\mathbb{Z}_p[X]$.

Proof. Sia n il numero di polinomi monici irriducibili di grado f. Notiamo che dal teorema precedente segue che, se f è primo, allora $x^{p^f} - x$ è ottenuto moltiplicando polinomi monici irriducibili il cui grado deve necessariamente essere 1 oppure f. Inoltre il grado di $x^{p^f} - x$ è p^f ed è ottenuto moltplicando n polinomi di grado f e p volte polinomi di grado 1. Uguagliando i grado troviamo la seguente relazione,

$$p^f = n * f + p \iff n = \frac{p^f - f}{f}$$

□