Appunti sui campi finiti.

Roberto Catenacci

Versione del 23 Novembre 2011

Nelle note sugli anelli abbiamo visto che per ogni primo p l'anello $\mathbb{Z}_p$ è un campo finito, esistono quindi campi finiti di con p elementi per ogni numero primo p. In queste dispense riassumiamo gli aspetti più elementari della teoria dei campi finiti dandone una descrizione abbastanza completa. Vedremo che per ogni primo p e per ogni intero positivo n esiste essenzialmente un unico campo con p^n elementi e si descriverà una procedura per costruirlo. Si può dimostrare anche abbastanza facilmente, ma noi non lo faremo in queste brevi note, che ogni corpo finito è commutativo e quindi è un campo. Questi due risultati concludono, in un certo senso, la teoria dei corpi finiti; partendo quasi da niente si può dare una descrizione semplice e completa di tutti i corpi finiti. Questioni simili, ad esempio: descrivere tutti gli anelli commutativi con identità oppure descrivere tutti i gruppi finiti, sono invece estremamente complesse e motivano (e hanno motivato) la ricerca di molti matematici da moltissimi anni.

Indice

1 Generalità sui campi finiti **2**

2 Estensioni di campi. **5**

3 Campo di spezzamento di un polinomio. **7**

4 Esistenza e unicità dei campi finiti. **8**

5 Automorfismi di un campo finito. **11**

6 Esempi e esercizi. **13**

1 Generalità sui campi finiti

Iniziamo con il seguente teorema importante che caratterizza il numero degli elementi di un campo finito:

Teorema 1.1 *Sia F_q un campo finito costituito da q elementi, allora $q = p^n$ per un certo primo p e F_q contiene un sottocampo F_p isomorfo a $\mathbb{Z}_p$.*

Prova. Essendo F_q finito deve esistere un naturale r tale che

$$r1 = 1 + \overset{r \text{ volte}}{1} + ... + 1 = 0. \tag{1}$$

Sia p il minimo di questi numeri; p deve essere primo, perchè se fosse composto, cioè $p = ab$ (con $a, b > 1$) per la distributività si avrebbe:

$$(\overset{a \text{ volte}}{1 + 1 + ... + 1}) \times (\overset{b \text{ volte}}{1 + 1 + ... + 1}) = (\overset{ab=p \text{ volte}}{1 + 1 + ... + 1}). \tag{2}$$

cioè:

$$0 = p1 = (ab)1 = a(b1) = (a1)(b1) \tag{3}$$

e questo, essendo F_q un campo, e quindi privo di divisori di zero, implicherebbe che almeno uno tra $a1$ e $b1$ sia $= 0$. Questo però è contrario all'ipotesi che p sia il minimo. Sia ora $F_p = \langle 1 \rangle$ il sottogruppo additivo generato da 1; è chiaramente un sottocampo e si ha immediatamente che F_p è isomorfo a $\mathbb{Z}_p$ (l'isomorfismo è $m1 \to \overline{m} \in \mathbb{Z}_p$). Allora (prendendo come operazioni la somma in F_q e come prodotto tra elementi di F_p e elementi di F_q il prodotto in F_q) F_q è chiaramente uno spazio vettoriale sul campo F_p. Essendo F_q finito, lo spazio è di dimensione finita (infatti ha certamente un insieme di generatori finito costituito dal campo stesso); siano n la dimensione e $\{x_1, ...x_n\}$ una base. Allora gli elementi di F_q sono del tipo:

$$x = a_1x_1 + ... + a_nx_n \tag{4}$$

con $a_i \in F_p$. Essendo $\#F_p = p$ si ricava che F_q ha p^n elementi. ■

Definizione 1.1 *F_p si dice sottocampo primo (o fondamentale) di F_q.*

Osservazione 1.1 *Chiaramente due campi con lo stesso numero di elementi hanno sottocampi primi isomorfi tra loro, perchè ambedue i sottocampi primi sono isomorfi a $\mathbb{Z}_p$. Questa è una delle ragioni fondamentali della semplicità della teoria dei campi finiti; dimostreremo infatti che ogni campo finito si ottiene estendendo in modo opportuno il suo sottocampo primo.*

Ci occupiamo ora dell'ordine (additivo e moltiplicativo) degli elementi di F_q. Sia $x \neq 0 \in F_q$ e denotiamo con $\#x$ l'ordine **additivo** (cioè rispetto alla somma) e con $@x$ l'ordine **moltiplicativo** (cioè rispetto al prodotto).

$$\#x = n \text{ se } n \text{ è il } \textbf{minimo} \text{ intero positivo per cui } nx = (\overset{n \text{ volte}}{x + x} + ... + x) = 0 \tag{5}$$

$$@x = n \text{ se } n \text{ è il } \textbf{minimo} \text{ intero positivo per cui } x^n = (\overset{n \text{ volte}}{x \cdot x} \cdot ... \cdot x) = 1 \tag{6}$$

Teorema 1.2 *Sia $x \neq 0 \in F_q$, allora $\#x = p$.*

Prova. Essendo F_q finito, ogni elemento ha ordine additivo finito. Siano $x, y \neq 0 \in F_q$ e sia: $\#x = r, \#y = s$, ovvero $rx = sy = 0$. Si ha quindi:

$$ry = r(xx^{-1}y) = (rx)(x^{-1}y) = 0 \tag{7}$$
$$sx = s(yy^{-1}x) = (sy)(y^{-1}x) = 0 \tag{8}$$

Osserviamo ora che abbiamo ottenuto:

$$rx = sx = 0 \Longrightarrow s \geq r \tag{9}$$
$$sy = ry = 0 \Longrightarrow r \geq s \tag{10}$$

e quindi $r = s$. Prendendo $y = 1$ otteniamo dal teorema precedente che $r = s = p$. ■

Definizione 1.2 *Il numero p si dice **caratteristica** di F_q e si denota $carF_q$. Si ha quindi: se $carF_q = p$, $\forall x \in F_q$, $px = 0$.*

Osservazione 1.2 *In un campo F_q con p^n elementi si ha:*

$$(x + y)^{p^n} = x^{p^n} + y^{p^n} \tag{11}$$

Ad esempio: se $carF_q = 2$ si ha:

$$(x + y)^2 = 2xy + x^2 + y^2 = x^2 + y^2 \tag{12}$$
$$(x + y)^3 = x^3 + y^3 + 3xy^2 + 3x^2y = x^3 + y^3 + xy^2 + x^2y \tag{13}$$
$$(x + y)^4 = x^4 + y^4 + 4xy^3 + 4x^3y + 6x^2y^2 = x^4 + y^4 \tag{14}$$

La formula si dimostra in generale scrivendo lo sviluppo del binomio.

Osservazione 1.3 *La nozione di caratteristica non richiede però che il campo sia finito. Se K è un campo, si dice che è **a caratteristica** 0 se la relazione $nk = 0$ (con n intero e $k \in K$) vale solo per $n = 0$. Esempi di campi a caratteristica 0 sono $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$. Se invece esiste un intero positivo n per cui $nk = 0$, per ogni $k \in K$, allora il campo si dice che è **a caratteristica** n. E' facile dimostrare (fatelo per esercizio) modificando opportunamente la dimostrazione del teorema precedente, che allora n deve essere un numero primo. **Ci sono campi infiniti di caratteristica finita.** Ad esempio, $\mathbb{Z}_p[x]$ è un dominio di integrità, e sia $\mathbb{F}(p)$ il suo campo delle frazioni (vedi le dispense sugli anelli): $\mathbb{F}(p)$ è infinito ed è a caratteristica p* [1].

[1] La teoria dei campi infiniti a caratteristica $\neq 0$ è complicata da fenomeni strani. Ad esempio, un polinomio in $\mathbb{R}[x]$ di secondo grado con una radice doppia è riducibile in $\mathbb{R}$, perchè la radice formale (ovvero a priori complessa) doppia deve necessariamente essere reale. Lo stesso è vero per $\mathbb{Q}$ e anche per $\mathbb{Z}_2$ ma non è vero ad esempio per il campo

$$K = \left\{\text{campo delle frazioni di } \mathbb{Z}_2\left[t^2\right]\right\} \subset K' = \{\text{campo delle frazioni di } \mathbb{Z}_2[t]\}$$

K e K' sono infiniti a caratteristica 2. Consideriamo il polinomio $p(x) = x^2 - t^2 \in K[x] : p(x)$ ha $t \in K'$ come radice formale doppia (in caratteristica 2 infatti $t = -t$) e quindi si fattorizza in K' come $(x+t)(x-t)$, ma non si fattorizza in K perchè è chiaro che $t \notin K$.

Occupiamoci ora dell'ordine moltiplicativo e dimostriamo il teorema più importante:

Teorema 1.3 *Il gruppo $F_q^* = F_q \setminus \{0\}$ delle unità di F_q è ciclico di ordine $p^n - 1$.*

Prova. Tutti gli elementi di F_q^* hanno ordine moltiplicativo finito, e denotiamo con m il massimo ordine possibile per gli elementi di F_q^*.

Consideriamo un elemento α con $@\alpha = m$ e il gruppo moltiplicativo $A = \langle \alpha \rangle$ generato da α. Allora $\#A = m$; vogliamo mostrare che $F_q^* = A$. Se $\alpha^i \in A$ si ha: $(\alpha^i)^m = (\alpha^m)^i = 1$ e quindi ogni elemento di A è una radice $\in F_q$ del polinomio $x^m - 1 \in F_q[x]$. Questo polinomio ha al più m radici in F_q [2]e quindi in A ci sono tutte le sue radici. Ogni $z \in F_q^*$ tale che $@z = n$ con n divisore di m deve stare in A perchè allora si ha: $z^m = z^{kn} = 1$ e quindi z è una radice di $x^m - 1$. Vogliamo ora mostrare che $F_q^* \setminus A$ è l'insieme vuoto. Sia $y \in F_q^* \setminus A$, necessariamente $@y = h$ non divide m e allora esiste un primo s tale che una sua potenza, s^i, divide h ma non m. Poniamo allora $h = s^i u$ e $m = s^j v$ con $0 \leq j < i$ e possiamo supporre che s non divida né u né v. Abbiamo allora:

$$1 = \alpha^m = \left(\alpha^{s^j}\right)^v \tag{15}$$

$$1 = y^h = (y^u)^{s^i} \tag{16}$$

Risulta allora che [3] $@\left(\alpha^{s^j}\right) = v$ e $@y^u = s^i$. Siccome poi v e s^i sono primi fra loro abbiamo (vedi ancora nota precedente):

$$@\left(y^u \alpha^{s^j}\right) = s^i \times v > s^j \times v = m \tag{17}$$

ma questo è assurdo perchè va contro la massimalità di m, e allora y non può esistere e quindi $F_q^* \setminus A = \emptyset$ e $F_q^* = A$. Essendo per costruzione A ciclico anche F_q^* lo è, in particolare si ha $m = p^n - 1$. ■

Definizione 1.3 *I generatori di F_q^* sono detti elementi primitivi.*

Osservazione 1.4 *Il teorema precedente assicura l'esistenza di elementi primitivi per ogni campo finito ed è perciò noto come* ***Teorema dell'elemento primitivo****. Il teorema però non è di carattere costruttivo e si sanno trovare in generale solo per tentativi. Uno dei pochi risultati noti è che se p è un primo della forma $4q+1$ con q primo, allora 2 è elemento primitivo*

[2]E' facile estendere a qualsiasi campo, usando il fatto che sostanzialmente le regole algebriche sono le stesse,buona parte dei risultati noti per i polinomi sul campo reale o complesso. Attenzione però che la **commutatività** è essenziale; ad esempio, nel corpo dei quaternioni, dato il polinomio di secondo grado $x^2 + 1$ possiamo scrivere subito almeno 3 radici: i, j e k.

[3]Ricordiamo le seguenti proprietà delle potenze degli elementi di un gruppo: sia g un elemento di ordine r allora:

1) $g^i = g^j \Leftrightarrow i = j \pmod r$

2) $@\left(g^i\right) = \frac{r}{MCD(i,r)}$

3) se h ha ordine s primo con r e se $gh = hg$ allora $@(gh) = @g \times @h$

di $\mathbb{Z}_p$ (ad esempio 2 è primitivo per $p = 5, 13, 29, ...$). C'è una congettura di Gauss che asserisce che 10 è elemento primitivo per infiniti primi. La congettura più nota è quella di Artin (1920): se n è un intero che non sia un quadrato allora è primitivo per $\mathbb{Z}_p$ per infiniti primi p. Tale congettura è stata poi dimostrata assumendo vera una generalizzazione della famosissima ipotesi di Riemann e questo fa capire come la natura degli elementi primitivi sia legata a uno dei più grandi problemi irrisolti della matematica.

Osservazione 1.5 *Il teorema dell'elemento primitivo può essere visto come un raffinamento del piccolo teorema di Fermat che asserisce che in un gruppo finito G, $\forall x \neq e$, $x^{\#G} = e$. Il teorema dell'elemento primitivo dice in più che in F_q^* esiste almeno un x di ordine massimale $@x = \#F_q^*$.*

Osservazione 1.6 *Una specie di inverso del teorema dell'elemento primitivo fornisce un **test di primalità**: sia n intero ≥ 2, se esiste un intero $a < n$ tale che $@a = n - 1$ in $\mathbb{Z}_n^*$ allora n è primo. Infatti se n non è primo $\varphi(n) < n - 1$ e ci sono due casi. Se a non è primo con n allora nessuna sua potenza può essere uguale a $1 \bmod n$, mentre se a è primo con n allora (per il teorema di Eulero) $@a \leq \varphi(n) < n - 1$. Quindi se $@a = n - 1$, n deve essere primo.*

2 Estensioni di campi.

Definizione 2.1 *Dato un campo E e un suo sottocampo F, si dice che E **è una estensione di** F.*

Definizione 2.2 *Un elemento $\alpha \in E$ si dice **algebrico** su F se esiste un polinomio $p(x) \in F[x]$ tale che $p(\alpha) = 0 \in E$.*

Definizione 2.3 *Se ogni elemento di E è algebrico su F, si dice che E **è una estensione algebrica di** F* [4].

Descriviamo ora una procedura con cui costruire estensioni algebriche.

Sia K un campo e consideriamo l'anello dei polinomi $K[x]$; siano $p(x)$ un polinomio **irriducibile** su K di grado d e $I = (p(x))$ l'ideale dei multipli di $p(x)$. Formiamo l'anello quoziente $\frac{K[x]}{(p(x))}$. I è costituito dai polinomi multipli di $p(x)$ e, equivalentemente, è l'insieme dei polinomi che divisi per $p(x)$ hanno resto zero. Sia ora $f(x) \in K[x]$, e dividiamolo per $p(x)$; si ottiene:

$$f(x) = q(x)p(x) + r(x) \tag{18}$$

La sua classe in $\frac{K[x]}{(p(x))}$, denotata da $\overline{f(x)}$ è l'insieme dei polinomi che divisi per $p(x)$ hanno lo stesso resto di $f(x)$, ovvero:

$$\overline{f(x)} = \overline{r(x)} = \overline{b_0 + b_1 x + ... + b_{d-1}x^{d-1}} \tag{19}$$

[4] Ad esempio, $\mathbb{C}$ è una estensione algebrica di $\mathbb{R}$; infatti ogni numero complesso α è radice del polinomio **reale** $x^2 - (\alpha + \overline{\alpha})x + \alpha\overline{\alpha}$.

Osserviamo ora che si ha un omomorfismo **iniettivo**

$$K \to \frac{K[x]}{(p(x))} \tag{20}$$

Infatti per $b \in K$, l'omomorfismo $f(b) = \overline{b}$ è iniettivo, perchè $\overline{a} = \overline{b} \Rightarrow a = q(x)p(x) + b$, ma $q(x) = 0$ perchè a e b sono o entrambi zero o di grado 0. **Possiamo allora identificare $\overline{b}$ con b.**

Definizione 2.4 *Si usa dire che l'anello $\frac{K[x]}{(p(x))}$ (dimostreremo più sotto che è un campo) è una* ***estensione semplice di*** *K e contiene come sottoanello una immagine isomorfa di K.*

Questa osservazione, unita alla definizione delle operazioni tra classi, ci consente di rappresentare ogni classe come:

$$\overline{f(x)} = \overline{r(x)} = \overline{b_0 + b_1 x + ... + b_{d-1}x^{d-1}} = b_0 + b_1\overline{x} + ... + b_{d-1}\overline{x^{d-1}} \tag{21}$$

Se $p(x) = a_0 + a_1 x + ... + a_d x^d$, essendo ovviamente $\overline{p(x)} = 0 = a_0 + a_1\overline{x} + ... + a_d\overline{x^d}$, ponendo ora $\overline{x} = \alpha$ si ottiene $p(\alpha) = 0$, ovvero α **è interpretabile come una radice di** $p(x)$**.** In altri termini, scrivendo gli elementi di $\frac{K[x]}{(p(x))}$ utilizzando α:

$$\frac{K[x]}{(p(x))} = \left\{ r(\alpha) = b_0 + b_1\alpha + ... + b_{d-1}\alpha^{d-1} \text{ con } b_i \in K \text{ e } p(\alpha) = 0 \right\} = K[\alpha] \tag{22}$$

Risulta che $K[\alpha]$ **è uno spazio vettoriale di dimensione** d **su** K perchè ogni suo elemento è una combinazione lineare a coefficienti in K degli elementi $\left\{1, \alpha, \alpha^2, ..., \alpha^{d-1}\right\}$ con inoltre la relazione $p(\alpha) = a_0 + a_1\alpha + ... + a_d\alpha^d = 0$.

Osservazione 2.1 ***Se*** *K* ***è un campo finito,*** *$K[\alpha]$* ***ha*** *k^d* ***elementi se*** *K* ***ne ha*** *k.*

Usiamo ora il fatto che $p(x)$ **è irriducibile** in K per dimostrare che $K[\alpha]$ **è un campo**.

Prova. Siccome $p(x)$ è irriducibile e ha grado d, $r(x)$, un possibile resto $\neq 0$, ha grado $< d$. Ne consegue che $p(x)$ e $r(x)$ non hanno fattori comuni. Esistono allora due altri polinomi $a(x)$ e $b(x)$ tali che

$$p(x)a(x) + r(x)b(x) = 1 \tag{23}$$

e quindi, valutando i polinomi su α e ricordando che $p(\alpha) = 0$:

$$r(\alpha)b(\alpha) = 1 \tag{24}$$

Si trova quindi che in $K[\alpha]$ ogni elemento diverso da zero ha inverso e quindi $K[\alpha]$ è un campo. ■

Osservazione 2.2 *I campi come $K[\alpha]$ ottenuti come estensioni semplici, ovvero aggiungendo a K una radice di un polinomio irriducibile su K sono* ***estensioni algebriche****, ovvero ogni elemento di $K[\alpha]$ è radice di un polinomio di $K[x]$.*

Prova. Sia $\beta \in K[\alpha]$. Essendo $K[\alpha]$ uno spazio vettoriale di dimensione d su K, i $d+1$ elementi $\left\{1, \beta, \beta^2, ..., \beta^d\right\}$ sono dipendenti e quindi esistono $d+1$ elementi non tutti nulli di K tali che:

$$c_0 + c_1\beta + ... + c_d\beta^d = 0 \tag{25}$$

Ovvero β è radice del polinomio $c_0 + c_1 x + ... + c_d x^d \in K[x]$. ■

3 Campo di spezzamento di un polinomio.

Teorema 3.1 *Sia K un campo e sia $f(x)$ un polinomio in $K[x]$ di grado $d \geq 1$. Allora esiste un campo F estensione di K tale che in $F[x]$ il polinomio $f(x)$ è scomponibile come prodotto di fattori di grado* 1.

Prova. La dimostrazione procede per induzione sul grado $\deg f(x) = d$ e il caso $d = 1$ è banale ($F = K$). Supponiamo allora che il grado di $f(x)$ sia $d > 1$; allora in $K[x]$ possiamo scomporre $f(x)$ in fattori irriducibili:

$$f(x) = p_1(x)p_2(x)...p_r(x) \tag{26}$$

Se per ogni i il grado di $p_1(x)$ è uguale a 1, abbiamo finito (ancora si ha $F = K$). Se no supponiamo che, ad esempio, il grado di $p_1(x)$ sia > 1. Costruiamo allora come nella sezione precedente il campo $K[\alpha] = \frac{K[x]}{(p_1(x))}$. Questo campo contiene K e una radice α di $p_1(x)$. Si può allora scomporre $p_1(x) = (x - \alpha)q_1(x)$ e il grado di $q_1(x)$ è $\deg p_1(x) - 1$. Allora in $K[\alpha]$ si ha:

$$f(x) = (x - \alpha)q_1(x)p_2(x)...p_r(x) = (x - \alpha)g(x) \tag{27}$$

Il polinomio $g(x)$ ha quindi grado $d-1$, e per l'ipotesi induttiva si fattorizza in fattori di primo grado in un campo F; e lo stesso vale quindi per il polinomio $f(x) = (x - \alpha)g(x)$. ■

Definizione 3.1 *Un campo F con le proprietà enunciate nel teorema si dice* ***campo di spezzamento*** *di $f(x)$.*

Esempio 3.1 *Consideriamo il polinomio $x^4 - x \in \mathbb{Z}_2[x]$. La sua scomposizione in fattori irriducibili è:*

$$x^4 - x = x(x^3 - 1) = x(x - 1)(x^2 + x + 1) \tag{28}$$

Il polinomio $x^2 + x + 1$ (pensato per un momento come polinomio di $\mathbb{C}[x]$) è il terzo polinomio ciclotomico e quindi le radici formali di $x^4 - x$ sono: $\{0, 1, \varepsilon, \varepsilon^2\}$ dove ε è una radice cubica primitiva di 1. *Si ha quindi che ε è un elemento primitivo: $\varepsilon^3 = 1$. Risulta allora che*

$$F_4 = \left\{0, 1, \varepsilon, \varepsilon^2\right\}$$

è un campo con le seguenti tavole di somma e moltiplicazione: (osservare che se ($\varepsilon^2 + \varepsilon + 1 = 0$ si ha, in $\mathbb{Z}_2[x]$, $\varepsilon^2 = -\varepsilon - 1 = \varepsilon + 1$)

$+$	$\mathbf{0}$	$\mathbf{1}$	ε	$\mathbf{1}+\varepsilon$
$\mathbf{0}$	0	1	ε	$1+\varepsilon$
$\mathbf{1}$	1	0	$1+\varepsilon$	ε
ε	ε	$1+\varepsilon$	0	1
$\mathbf{1}+\varepsilon$	$1+\varepsilon$	ε	1	0

$\cdot$	$\mathbf{0}$	$\mathbf{1}$	ε	$\mathbf{1}+\varepsilon$
$\mathbf{0}$	0	0	0	0
$\mathbf{1}$	0	1	ε	$1+\varepsilon$
ε	0	ε	$1+\varepsilon$	1
$\mathbf{1}+\varepsilon$	0	$1+\varepsilon$	1	ε

Si verifica subito che F_4 è un campo di spezzamento di $x^4 - x$ che infatti, in F_4, si scompone in polinomi di primo grado:

$$x^4 - x = x(x - 1)(x - \varepsilon)(x - \varepsilon^2)$$

Teorema 3.2 *Sia F un campo di spezzamento di $x^q - x \in \mathbb{Z}_p[x]$ con $q = p^n$. La scomposizione di $f(x)$ in $F[x]$ non ha fattori ripetuti.*

Prova. Ricordiamo che per i polinomi reali o complessi una radice multipla è tale se è radice del polinomio e della sua derivata prima. Ciò è vero anche per i polinomi su campi finiti perchè le regole formali della divisione con resto e della derivazione di polinomi si possono applicare anche in questo caso. La derivata formale di $x^q - x$ è $qx^{q-1} - 1$ ma in $\mathbb{Z}_p[x]$ si ha:

$$qx^{q-1} = \overset{q \text{ volte}}{x^{q-1} + x^{q-1} + ... + x^{q-1}} = 0 \tag{29}$$

Perchè $q = p^n$ e in $\mathbb{Z}_p$ si ha $py = 0\ \forall y$. Quindi $x^q - x \in \mathbb{Z}_p[x]$ ha solo radici semplici in $F[x]$ perchè la sua derivata prima formale vale sempre -1. Ne consegue che ha esattamente $q = p^n$ radici. ■

4 Esistenza e unicità dei campi finiti.

La costruzione descritta nel paragrafo precedente è molto importante perchè risulta essere - universale nel senso che qualsiasi campo finito K è isomorfo a un campo del tipo $\mathbb{Z}_p[\alpha]$ ovvero è una estensione semplice algebrica di $\mathbb{Z}_p$. Diamo prima un teorema di struttura

Teorema 4.1 ***Teorema di struttura.*** *Sia K un campo finito con k elementi e a caratteristica p; allora è isomorfo a una estensione semplice $\mathbb{Z}_p[\alpha] = \frac{\mathbb{Z}_p[x]}{(p(x))}$ (dove $p(x)$ è irriducibile)*

Prova. Sappiamo che K ha un elemento primitivo α che, essendo di ordine $k-1$,è radice di $x^{k-1} - 1 \in F_p[x] \approx \mathbb{Z}_p[x]$ (dove F_p è il sottocampo primo di K). Sia $p(x) \in \mathbb{Z}_p[x]$ il polinomio monico di minimo grado tale che $p(\alpha) = 0$; $p(x)$ è irriducibile in $\mathbb{Z}_p[x]$ ed è detto **polinomio minimo**[5]. L'applicazione: $\Phi : \frac{\mathbb{Z}_p[x]}{(p(x))} \to K$ definita da:

$$\Phi\left(\overline{f(x)}\right) = r(\alpha) \tag{30}$$

dove stiamo usando le notazioni della precedente sezione, è l'isomorfismo cercato: infatti è ben definita $\left(\overline{f(x)} = \overline{r(x)}\right)$, è un omomorfismo di anelli, è iniettiva perchè ha nucleo banale ($\frac{\mathbb{Z}_p[x]}{(p(x))}$ è un campo e quindi non ha ideali non banali e sappiamo che il nucleo di un omomorfismo di anelli è un ideale) ed è anche suriettiva perchè $\Phi\left(\overline{0}\right) = 0$, $\Phi\left(\overline{x^i}\right) = \alpha^i$ e ogni elemento di K è una qualche potenza di α. ■

Osservazione 4.1 *Si pone ora la questione dell'esistenza: sappiamo che un campo finito con k elementi e a caratteristica p deve avere $k = p^n$ elementi e che è isomorfo a una estensione semplice algebrica di $\mathbb{Z}_p$, ma ancora resta da dimostrare che per ogni $k = p^n$ esiste un campo di k elementi.*

[5] $p(x)$ esiste perchè un elemento primitivo α è algebrico su $\mathbb{Z}_p[x]$, essendo radice di $x^{k-1} - 1 \in F_p[x] \approx \mathbb{Z}_p[x]$. Se $p(x)$ fosse riducibile, cioè $p(x) = a(x)b(x)$, si avrebbe $a(\alpha)b(\alpha) = 0$, ma allora, essendo K un campo, $a(\alpha) = 0$ oppure $b(\alpha) = 0$ e quindi $p(x)$ non sarebbe di grado minimo. Nella sezione di esercizi e esempi diamo una procedura per costruire polinomi minimi.

Teorema 4.2 ***Teorema di esistenza.*** *Dati un primo p e un intero n, esiste un campo F_q con $q = p^n$ elementi.*

Prova. Consideriamo il polinomio $x^q - x \in \mathbb{Z}_p[x]$ con $q = p^n$, e un suo campo di spezzamento F. Sia

$$F_q = \{\text{tutte le radici di } x^q - x \text{ in } F\} = \{a \in F \text{ tali che } a^q = a\} \subset F \tag{31}$$

Sappiamo (vedi l'ultimo teorema della precedente sezione) che l'insieme $F_q \subset F$ ha $q = p^n$ elementi. Dobbiamo ora dimostrare che è un campo:

- $0, 1 \in F_q$
- se $a, b \in F_q$, $(a+b)^{p^n} = a^{p^n} + b^{p^n} = a + b$ (vedi la formula 11) e $(a \cdot b)^{p^n} = a^{p^n} \cdot b^{p^n} = a \cdot b$
- se $a \neq 0 \in F_q$, $a^{-1} \in F_q$: infatti $(a^{-1})^{p^n} = \left(a^{p^n}\right)^{-1} = a^{-1}$
- se $a \in F_q$, si ha poi: $0 = (a + (-a))^{p^n} = a^{p^n} + (-a)^{p^n}$ cioè $0 = a + (-a)^{p^n}$ e quindi $(-a)^{p^n} = -a$

■

Osservazione 4.2 ***Il teorema precedente dice anche che esiste in*** $Z_p[x]$ ***un polinomio*** $p(x)$ ***irriducibile di grado*** n ***arbitrario.*** *Infatti consideriamo F_{p^n} ; per il teorema di struttura è isomorfo a una estensione semplice $\frac{\mathbb{Z}_p[x]}{(p(x))}$ e $p(x)$ quindi è irriducibile di grado n.* ***Inoltre si ricava che*** $p(x)$ ***divide*** $x^q - x$*, infatti se così non fosse esisterebbero due polinomi $a(x)$ e $b(x)$ tali che:*

$$1 = p(x)a(x) + (x^q - x)\, b(x)$$

Se β è una radice di $p(x)$ in $\frac{\mathbb{Z}_p[x]}{(p(x))}$, $\beta^q = \beta$ per il piccolo teorema di Fermat, e quindi $\beta \in F_q$. Si avrebbe allora un assurdo:

$$1 = p(\beta)a(\beta) + (\beta^q - \beta)\, b(\beta) = 0$$

Osservazione 4.3 ***Il campo*** F_q ***costruito nel teorema precedente è minimale e quindi unico nel senso che, per costruzione, è il più piccolo campo che contiene*** Z_p ***e tutte le radici di*** $x^q - x$*.*

Il teorema precedente ci dice anche che:

$$x^{q-1} - 1 = \prod_{a \in F_q^*} (x - a) \tag{32}$$

$$x^q - x = \prod_{a \in F_q} (x - a) \tag{33}$$

Ponendo $x = 0$ otteniamo dalla prima formula

$$-1 = \prod_{a \in F_q^*} (-a) = (-1)^{q-1} \prod_{a \in F_q^*} a = \prod_{a \in F_q^*} a$$

Infatti se q è dispari abbiamo $-1 = \prod_{a \in F_q^*} a$, se q è pari abbiamo ancora lo stesso risultato perchè in caratteristica 2 si ha che $1 = -1$.

Possiamo ora concludere la teoria con il teorema di unicità.

Teorema 4.3 ***Teorema di unicità.*** *Ogni campo finito K di ordine $q = p^n$ è isomorfo a F_q. Ovvero, due campi finiti dello stesso ordine sono isomorfi.*

Prova. Sappiamo per il teorema di struttura che K di ordine $q = p^n$ (che esiste per il teorema di esistenza) è isomorfo a una estensione semplice $\frac{\mathbb{Z}_p[x]}{(p(x))}$ con $p(x)$ irriducibile di grado n. Se α è una radice di $p(x)$ in $\frac{\mathbb{Z}_p[x]}{(p(x))}$, sappiamo dall'osservazione precedente che $p(x)$ **divide** $x^q - x$, quindi $\alpha \in F_q$. L'applicazione: $\Phi : \frac{\mathbb{Z}_p[x]}{(p(x))} \to F_q$ definita da:

$$\Phi\left(\overline{f(x)}\right) = r(\alpha) \tag{34}$$

dove stiamo usando le notazioni della precedente sezione, è l'isomorfismo cercato: infatti è **ben definita** $\left(\overline{f(x)} = \overline{r(x)}\right)$, è un **omomorfismo** di anelli, è **iniettiva** perchè ha nucleo banale ($\frac{\mathbb{Z}_p[x]}{(p(x))}$ è un campo e quindi non ha ideali non banali e sappiamo che il nucleo di un omomorfismo di anelli è un ideale) ed è anche **suriettiva** perchè $\frac{\mathbb{Z}_p[x]}{(p(x))}$ e F_q hanno lo stesso numero di elementi. Abbiamo allora la catena di isomorfismi:

$$K \approx \frac{\mathbb{Z}_p[x]}{(p(x))} \approx F_q$$

■

Osservazione 4.4 *Osserviamo che dal teorema precedente discende immediatamente che $\frac{\mathbb{Z}_p[x]}{(p(x))} \approx \frac{\mathbb{Z}_p[x]}{(q(x))}$ se e solo se $p(x)$ e $q(x)$ sono irriducibili dello stesso grado, e che la scelta della radice α di $p(x)$ con cui costruire $\mathbb{Z}_p[\alpha]$ è ininfluente. Non sempre, anche se potrebbe essere utile nei calcoli, si può prendere come α una radice primitiva, ovvero un elemento primitivo di $\mathbb{Z}_p[\alpha]$. Un polinomio irriducibile di grado n che ha una radice primitiva (ovvero che è un elemento primitivo di F_{p^n}) è detto polinomio primitivo. Non tutti i polinomi irriducibili sono polinomi primitivi (vedi nella sezione di esempi e esercizi) e determinare se un polinomio irriducibile è primitivo può essere un problema piuttosto difficile.*

5 Automorfismi di un campo finito.

Un automorfismo di un campo è un isomorfismo di un campo in sé stesso. L'insieme degli automorfismi di un campo è un gruppo con la composizione.

Teorema 5.1 *Sia F_q un campo finito di cardinalità $q = p^n$, l'applicazione $\sigma : F_q \to F_q$ definita da:*

$$\sigma(x) = x^p \tag{35}$$

è un automorfismo di F_q, detto ***automorfismo di Frobenius.*** *Inoltre, σ ha ordine n nel gruppo degli automorfismi.*

Prova. L'applicazione σ è un omomorfismo per le formule note:

$$(x+y)^p = x^p + y^p, (xy)^p = x^p y^p, 1^p = 1 \tag{36}$$

è iniettivo perchè il dominio è un campo ed è suriettivo perchè dominio e codominio coincidono e sono insiemi finiti.

Sia ora α un elemento primitivo di F_q ovvero un generatore di F_q^*; abbiamo che $\sigma^k(x) = x$ $\forall x \in F_q$ se e solo se $\sigma^k(\alpha) = \alpha^{p^k} = \alpha$, ovvero, essendo ovviamente $\alpha \neq 0$, $\alpha^{p^k - 1} = 1$. L'ordine di α è però $p^n - 1$ e quindi il minimo k possibile è $k = n$. ■

Osservazione 5.1 *L'insieme dei punti fissi di σ, ovvero l'insieme degli elementi tali che $\sigma(x) = x$ è ovviamente (per il piccolo teorema di Fermat) il sottocampo primo $F_p = \mathbb{Z}_p$.*

Osservazione 5.2 ***Ogni automorfismo φ di F_q fissa F_p.*** *Infatti:*

$$\varphi(1) = 1 \Rightarrow \varphi(1+1) = 1+1 \text{ e così via.} \tag{37}$$

Definizione 5.1 *Si definisce* ***gruppo di Galois*** *di F_q su F_p, e si denota con $Gal\,(F_q : F_p)$ l'insieme degli automorfismi di F_q.*

Osservazione 5.3 *Ricordando che F_q è una estensione di F_p, di grado n, generalizzando si può considerare una estensione di grado m, F_{q^m} di F_q e definire, corrispondentemente, il* ***gruppo di Galois*** *di F_{q^m} su F_q, $Gal\,(F_{q^m} : F_q)$ come l'insieme degli automorfismi di F_{q^m}* ***che fissano il sottocampo*** *F_q. E' facile verificare che $Gal\,(F_{q^m} : F_q)$ è effettivamente un sottogruppo del gruppo degli automorfismi di F_{q^m}.*

Studiamo ora, come semplice introduzione alla teoria di Galois, il gruppo $Gal\,(F_q : F_p)$.

Teorema 5.2 ***Lemma di Dedekind.*** *Siano σ_i con $i = 1...m$ automorfismi di un campo K distinti fra loro; allora sono indipendenti, ovvero:*

$$a_1\sigma_1(x) + a_2\sigma_2(x) + ... + a_m\sigma_m(x) = 0 \ \forall x \in K^* \Rightarrow a_i = 0 \in K \tag{38}$$

Prova. Si dimostra per induzione. E' vero per $n = 1$. Consideriamo ora $y \in K^*$:

$$a_1\sigma_1(xy) + ...a_m\sigma_m(xy) = 0 \Rightarrow a_1\sigma_1(x)\sigma_1(y) + a_2\sigma_2(x)\sigma_2(y) + ...a_m\sigma_m(x)\sigma_m(y) = 0 \quad (39)$$

$$a_1\sigma_1(x) + ...a_m\sigma_m(x) = 0 \Rightarrow a_1\sigma_1(x)\sigma_1(y) + a_2\sigma_2(x)\sigma_1(y) + ...a_m\sigma_m(x)\sigma_1(y) = 0 \quad (40)$$

Sottraendo otteniamo:

$$a_2\sigma_2(x)[\sigma_2(y) - \sigma_1(y)] + ... + a_m\sigma_m(x)[\sigma_m(y) - \sigma_1(y)] = 0 \quad (41)$$

Allora per l'ipotesi induttiva deve essere:

$$a_i[\sigma_i(y) - \sigma_1(y)] = 0,\ i = 2...m \quad (42)$$

Questo implica che $a_i = 0$, $i = 2...m$, perchè altrimenti almeno un $\sigma_i(y)$ coinciderebbe con $\sigma_1(y)$ per ogni y e questo è impossibile perchè i σ_i sono supposti distinti. Segue allora che necessariamente anche $a_1 = 0$. ■

Teorema 5.3 *Sia K una estensione finita di un campo F di grado k, allora $\#Gal(K : F) \leq k$*

Prova. Sia u_i, $1 = 1...k$ una base di K su F. Supponiamo che ci siano $k + 1$ automorfismi distinti in $Gal(K : F)$. Consideriamo il siatema lineare omogeneo di k equazioni e $k + 1$ incognite:

$$x_1\sigma_1(u_1) + x_2\sigma_2(u_1) + ... + x_{k+1}\sigma_{k+1}(u_1) = 0 \quad (43)$$

$$..... = 0 \quad (44)$$

$$x_1\sigma_1(u_k) + x_2\sigma_2(u_k) + ... + x_{k+1}\sigma_{k+1}(u_k) = 0 \quad (45)$$

Questo sistema ha sempre una soluzione non banale (ovvero diversa dalla soluzione nulla) a_i $i = 1...k + 1$ infatti è omogeneo e il numero di incognite supera il numero di equazioni; allora il sistema ha ∞^{k+1-r} soluzioni e il rango r della matrice dei coefficienti può essere al massimo k . Allora, per $i = 1...k + 1$, si ha:

$$a_1\sigma_1(u_i) + a_2\sigma_2(u_i) + ... + a_{k+1}\sigma_{k+1}(u_i) = 0 \quad (46)$$

Ogni elemento x di K si scrive $x = b_1u_1 + ... + b_ku_k$ con $b_i \in F$. Otteniamo allora, moltiplicando per b_i e ricordando che ogni $\sigma_i \in Gal(K : F)$ lascia fisso ogni elemento di F :

$$b_ia_1\sigma_1(u_i) = a_1\sigma_1(b_i)\sigma_1(u_i) = a_1\sigma_1(b_iu_i) \quad (47)$$

Per cui:

$$b_ia_1\sigma_1(u_i) + b_ia_2\sigma_2(u_i) + ... + b_ia_{k+1}\sigma_{k+1}(u_i) = a_1\sigma_1(b_iu_i) + a_2\sigma_2(b_iu_i) + ... + a_{k+1}\sigma_{k+1}(b_iu_i) = 0 \quad (48)$$

Sommando su i si ottiene quindi:

$$a_1\sigma_1(x) + a_2\sigma_2(x) + ... + a_{k+1}\sigma_{k+1}(x) = 0 \quad (49)$$

e questo contraddice il lemma di Dedekind (per $m = k + 1$). ■

Teorema 5.4 *$Gal\,(F_q : F_p)$ è un gruppo ciclico di ordine n; un suo generatore è l'omomorfismo di Frobenius σ.*

Prova. Basta applicare il teorema precedente all'estensione finita di grado n data da $K = F_q, F = F$. Si ottiene $\#Gal\,(F_q : F_p) \leq n$ e poi osservare che $\#Gal\,(F_q : F_p)$ contiene un elemento di ordine n (l'omomorfismo di Frobenius σ). ■

Osservazione 5.4 *Molte parti importanti della teoria riassunta in questi appunti si estendono al caso di campi infiniti e costituiscono la base della cosiddetta teoria di Galois che tratta in generale delle estensioni e degli automorfismi dei campi, argomenti di un corso più avanzato di algebra.*

Osservazione 5.5 *La teoria dei campi finiti trova la sua più rilevante applicazione pratica in informatica, principalmente nella costruzione dei metodi di rilevamento e correzione di errori di trasmissione (teoria dei codici).*

6 Esempi e esercizi.

Sia $Z_2\,[x]$ l'anello dei polinomi in x a coefficienti in Z_2.

- Mostrare che non ha divisori dello zero. E' un campo?
- Fattorizzare in polinomi di primo grado il polinomio $x^2 + 1$.
- Mostrare che il polinomio $x^2 + x + 1$ non ha radici in $\mathbb{Z}_2$.
- Sia ε una radice complessa di $x^2 + x + 1$ e si consideri l'insieme:

$$\mathbb{F} = \left\{a + \varepsilon b \text{ con } a, b \in \mathbb{Z}_2\ ,\ \varepsilon^2 + \varepsilon + 1 = 0\right\} \tag{50}$$

  con le due operazioni:

$$(a + \varepsilon b) + (c + \varepsilon d) = (a + c) + \varepsilon\,(b + d) \tag{51}$$
$$(a + \varepsilon b)\,(c + \varepsilon d) = (ac + bd) + \varepsilon\,(ad + bc + bd) \tag{52}$$

- Scrivere le tavole delle due operazioni e concludere che è un campo.
- Mostrare che rispetto alla somma $\mathbb{F}$ non è un gruppo ciclico.
- Mostrare che invece rispetto alla moltiplicazione $\mathbb{F}^* = \mathbb{F} \setminus \{0\}$ è un gruppo ciclico e darne un generatore.
- Mostrare che $\mathbb{F} = \frac{\mathbb{Z}_2[x]}{(x^2+x+1)}$ dove $(x^2 + x + 1)$ è l'ideale generato dal polinomio irriducibile

$$x^2 + x + 1$$

Soluzione:

- $\mathbb{Z}_2[x]$ non ha divisori dello zero perchè i coefficienti sono in un campo. Non è un campo perchè l'unico elemento invertibile è 1
- $x^2+1=(x+1)(x+1)$.
- La funzione x^2+x+1 assume solo il valore 1.
- Gli elementi dell'insieme sono $0, 1, \varepsilon, 1+\varepsilon$ e le tavole delle operazioni sono:

$$\left|\begin{array}{ccccc} + & \mathbf{0} & \mathbf{1} & \varepsilon & \mathbf{1}+\varepsilon \\ \mathbf{0} & 0 & 1 & \varepsilon & 1+\varepsilon \\ \mathbf{1} & 1 & 0 & 1+\varepsilon & \varepsilon \\ \varepsilon & \varepsilon & 1+\varepsilon & 0 & 1 \\ \mathbf{1}+\varepsilon & 1+\varepsilon & \varepsilon & 1 & 0 \end{array}\right| \quad \left|\begin{array}{ccccc} \cdot & \mathbf{0} & \mathbf{1} & \varepsilon & \mathbf{1}+\varepsilon \\ \mathbf{0} & 0 & 0 & 0 & 0 \\ \mathbf{1} & 0 & 1 & \varepsilon & 1+\varepsilon \\ \varepsilon & 0 & \varepsilon & 1+\varepsilon & 1 \\ \mathbf{1}+\varepsilon & 0 & 1+\varepsilon & 1 & \varepsilon \end{array}\right|$$

- E' un campo perchè è un anello commutativo con unità ed inoltre ogni elemento diverso da zero ha un *inverso.*
- $\mathbb{F}$ ha ordine 4, ma non ha elementi di ordine 4, infatti tutti i suoi elementi hanno ordine 2 rispetto alla somma.
- $\mathbb{F}^* = \mathbb{F}\setminus\{0\}$ ha ordine 3, un generatore è ad esempio, ε che ha ordine 3 rispetto al prodotto.
- In $\mathbb{F} = \frac{\mathbb{Z}_2[x]}{(x^2+x+1)}$ ogni classe è rappresentata da $\overline{a+bx}$, essendo $a+bx$ il resto della divisione di qualsiasi polinomio per x^2+x+1. Basta verificare che la somma e il prodotto tra classi sono gli stessi definiti più sopra da:

$$(a+\varepsilon b)+(c+\varepsilon d)=(a+c)+\varepsilon(b+d) \tag{53}$$
$$(a+\varepsilon b)(c+\varepsilon d)=(ac+bd)+\varepsilon(ad+bc+bd) \tag{54}$$

Per la somma è ovvio, per il prodotto si ha:

$$\left(\overline{a+bx}\right)\left(\overline{c+dx}\right)=\overline{(a+bx)(c+dx)}=\overline{ac+(ad+bc)x+bdx^2} \tag{55}$$

ma essendo (ricordando che in $\mathbb{Z}_2$ ogni elemento ha ordine 2 ripetto alla somma):

$$ac+(ad+bc)x+bdx^2=ac+bd+(ad+bc+bd)x+bd\left(x^2+x+1\right) \tag{56}$$

si ottiene il risultato voluto:

$$\left(\overline{a+bx}\right)\left(\overline{c+dx}\right)=\overline{ac+bd+x(ad+bc+bd)} \tag{57}$$

Un isomorfismo tra $\mathbb{F}$ e $\frac{\mathbb{Z}_2[x]}{(x^2+x+1)}$ è dato da $(a+\varepsilon b)\to\left(\overline{a+bx}\right)$.

Un esempio con un campo infinito.
Sia $\omega \neq 1$ una radice cubica complessa di 1 e sia $Z[\omega] = \{a + \omega b \mid a, b \in \mathbb{Z}\}$

- Mostrare che ω soddisfa l'equazione $\omega^2 + \omega + 1 = 0$
- Mostrare che $\mathbb{Z}[\omega]$ è un anello commutativo con indentità definendo in $\mathbb{Z}[\omega]$ una somma e un prodotto naturali.
- Mostrare che i sei elementi $\pm 1, \pm\omega, \pm(1+\omega)$ sono unità dell'anello $\mathbb{Z}[\omega]$
- Mostrare che $G = \{\pm 1, \pm\omega, \pm(1+\omega)\}$ con il prodotto definito in $\mathbb{Z}[\omega]$ è un gruppo abeliano ciclico.
- Mostrare esplicitamente, scrivendo un isomorfismo, che G è isomorfo a $\mathbb{Z}_6$.
- Trovare[6] $\mathbb{Z}[\omega]^*$ cioè il gruppo degli elementi invertibili di $\mathbb{Z}[\omega]$.
- Mostrare che ogni $z = a + \omega b \in \mathbb{Z}[\omega]$ è radice del polinomio $z^2 - (2a - b)z + (a^2 - ab + b^2)$
- Mostrare che $\mathbb{Z}[\omega]$ è isomorfo a $\frac{\mathbb{Z}[x]}{(x^2+x+1)}$ dove $(x^2 + x + 1)$ è l'ideale generato dal polinomio $x^2 + x + 1$.

Soluzione:

- $\omega^3 = 1$ per cui abbiamo:

$$S = 1 + \omega + \omega^2 = \omega + \omega^2 + \omega^3 = \omega(1 + \omega + \omega^2) = \omega S$$

essendo $\omega \neq 1$ segue $S = 0$

- Le operazioni naturali sono:

$$(a + \omega b) + (c + \omega d) = (a + c) + \omega\,(b + d) \tag{58}$$
$$(a + \omega b) \cdot (c + \omega d) = ac + ad\omega + bc\omega + bd\omega^2 = \tag{59}$$
$$ac + ad\omega + bc\omega + bd(-1 - \omega) = ac - bd + \omega\,(ad + bc - bd) \tag{60}$$

queste operazioni sono interne all'insieme e commutative, gli elementi neutri sono rispettivamente $0, 1$.

- Gli elementi dati sono invertibili, infatti:

$$(\pm 1)^{-1} = \pm 1$$
$$(\pm\omega)^{-1} = \pm\omega^2 = \mp(1 + \omega) \quad \text{(ricordando che } \omega^3 = 1)$$

[6] Per risolvere questo punto usare il fatto che le uniche soluzioni **intere** dell'equazione $a^2 + b^2 - ab = 1$ sono: $a = \pm 1, b = 0$; $a = 0, b = \pm 1$; $a = b = \pm 1$. Invece l'equazione $a^2 + b^2 - ab = -1$ non ammette soluzioni intere.
Questo può essere dimostrato facilmente risolvendo esplicitamente ad esempio per l'incognita a e analizzando le condizioni per cui le soluzioni siano intere.

- Il gruppo G è ciclico di ordine 6, infatti si trova subito che, ad esempio, $-\omega$ è un generatore:

$$\begin{aligned}
(-\omega)^1 &= -\omega \\
(-\omega)^2 &= \omega^2 = -1-\omega \\
(-\omega)^3 &= -\omega^3 = -1 \\
(-\omega)^4 &= \omega^4 = \omega^3\omega = \omega \\
(-\omega)^5 &= -\omega^5 = -\omega^3\omega^2 = -\omega^2 = 1+\omega \\
(-\omega)^6 &= \omega^6 = \left(\omega^3\right)^2 = 1
\end{aligned}$$

- Un isomorfismo $f : \mathbb{Z}_6 \to \mathbb{Z}[\omega]$ si ottiene, ad esempio, mandando il generatore 1 nel generatore $-\omega$: $f(n) = (-\omega)^n$ con $n = 0, 1, 2, 3, 4, 5$

- Si consideri l'equazione:

$$(a+\omega b)\cdot(x+\omega y) = ax - by + \omega\,(ay + bx - by) = 1 \tag{61}$$

  Con a, b interi non contemporaneamente nulli. Si ottiene il sistema:

$$\begin{aligned}
ax - by &= 1 \\
(ay + bx - by) &= 0
\end{aligned}$$

  dove deve essere anche $a, b, x, y \in \mathbb{Z}$. Il sistema ammette le soluzioni formali:

$$\begin{aligned}
x &= \frac{a-b}{a^2+b^2-ab} \\
y &= \frac{-b}{a^2+b^2-ab}
\end{aligned}$$

  Il denominatore non può mai essere zero se $a, b \in \mathbb{Z}$ e non contemporaneamente nulli (verificare risolvendo esplicitamente l'equazione $a^2+b^2-ab = 0$ come equazione di secondo grado in a). Ci sono ora tre casi.

- Se $b = 0$, $y = 0$ e affinchè anche x sia intero deve essere $a = \pm 1$ e quindi ± 1 sono elementi invertibili.

- Se $a = 0$, $x = y = -\frac{1}{b}$ e allora affinchè x e y siano interi deve essere $b = \pm 1$ e quindi $\pm\omega$ sono elementi invertibili con inversi rispettivamente $\mp(1+\omega)$

- Se a e b sono ambedue diversi da zero, affinchè x e y siano interi deve essere $a^2+b^2-ab = 1$ oppure $a^2+b^2-ab = -1$ (che però è impossibile). In questo caso risulta $a^2+b^2-ab-1 = 0$, le cui soluzioni formali (ad esempio per a) sono:

$$\frac{1}{2}b - \frac{1}{2}\sqrt{4-3b^2},\ \frac{1}{2}b + \frac{1}{2}\sqrt{4-3b^2}$$

  E queste sono intere (cioè vere soluzioni) solo per $b = \pm 1$ che a sua volta fornisce $a = \pm 1$. Risulta quindi che $\pm(1+\omega)$ sono elementi invertibili.

- Riassumendo, non essendoci altri casi, gli elementi invertibili sono solo

$$\{\pm 1, \pm\omega, \pm(1+\omega)\}$$

- In $\frac{\mathbb{Z}[x]}{(x^2+x+1)}$ ogni classe è rappresentata da $\overline{a+bx}$, essendo $a+bx$ il resto della divisione di qualsiasi polinomio per x^2+x+1. Basta verificare che la somma e il prodotto tra classi sono gli stessi definiti più sopra da:

$$(a+\omega b)+(c+\omega d) = (a+c)+\omega\,(b+d) \tag{62}$$
$$(a+\omega b)\cdot(c+\omega d) = ac-bd+\omega\,(ad+bc-bd) \tag{63}$$

  Per la somma è ovvio, per il prodotto si ha:

$$\left(\overline{a+bx}\right)\left(\overline{c+dx}\right) = \overline{(a+bx)\,(c+dx)} = \overline{ac+(ad+bc)\,x+bdx^2} \tag{64}$$

  ma essendo:

$$ac+(ad+bc)\,x+bdx^2 = (x^2+x+1)bd+(ad+bc-bd)\,x+ac-bd \tag{65}$$

  si ottiene il risultato voluto:

$$\left(\overline{a+bx}\right)\left(\overline{c+dx}\right) = \overline{ac-bd+x\,(ad+bc-bd)}$$

Sia $Z_3[x]$ l'anello dei polinomi a coefficienti in Z_3.

- Mostrare che non ha divisori dello zero. E' un campo?
- Fattorizzare in polinomi di primo grado il polinomio x^2+2.
- Mostrare che il polinomio x^2-2 non ha radici in $\mathbb{Z}_3$.
- Sia ε una soluzione formale di x^2-2 e si consideri l'insieme:

$$\mathbb{F} = \left\{a+\varepsilon b \text{ con } a,b\in\mathbb{Z}_3\ ,\ \varepsilon^2=2\right\} \tag{66}$$

  con le due operazioni:

$$(a+\varepsilon b)+(c+\varepsilon d) = (a+c)+\varepsilon\,(b+d) \tag{67}$$
$$(a+\varepsilon b)\,(c+\varepsilon d) = (ac+2bd)+\varepsilon\,(ad+bc) \tag{68}$$

  mostrare che è un campo.

- Mostrare che, rispetto alla somma, $\mathbb{F}$ non è un gruppo ciclico.
- Mostrare che invece rispetto alla moltiplicazione $\mathbb{F}^* = \mathbb{F}\setminus\{0\}$ è un gruppo ciclico, generato da $1+\varepsilon$.

- Mostrare che $\mathbb{F} = \frac{\mathbb{Z}_3[x]}{(x^2-2)}$ dove (x^2-2) è l'ideale generato dal polinomio x^2-2.

Soluzione:

- $\mathbb{Z}_3[x]$ non ha divisori dello zero perchè i coefficienti sono in un campo. Non è un campo perchè gli unici elementi invertibili sono 1 e 2.
- $x^2+2 = (x+1)(x+2)$.
- La funzione x^2-2 assume solo i valori 1 e 2
- E' un campo perchè è un anello commutativo con unità ed inoltre si mostra che ogni elemento diverso da zero ha un *inverso*. Si consideri il prodotto:

$$(a+\varepsilon b)(a-\varepsilon b) = a^2 - 2b^2 \tag{69}$$

In $\mathbb{Z}_3$, se $a \neq 0$ e $b \neq 0$, si ha $a^2 - 2b^2 = 1 - 2 = -1$ (in virtù del teorema di Fermat) e quindi ogni elemento con $a \neq 0$ e $b \neq 0$ ha un inverso:

$$(a+\varepsilon b)^{-1} = -a + \varepsilon b \tag{70}$$

Gli altri elementi diversi da zero hanno invece come inversi: $a^{-1} = a$ e $(\varepsilon b)^{-1} = 2\varepsilon b$, infatti $a^2 = 1$ e $(\varepsilon b)(2\varepsilon b) = 4b^2 = 1$ ancora per Fermat.

- $\mathbb{F}$ ha ordine 9, ma non ha elementi di ordine 9, infatti per tutti i suoi elementi si ha: $3(a+\varepsilon b) = 0$.
- $\mathbb{F}^* = \mathbb{F} \setminus \{0\}$ ha ordine 8, e quindi basta trovare un elemento di ordine 8. Osserviamo che ε ha ordine 4 e che $(1+\varepsilon)^2 = 2\varepsilon$ e quindi $(1+\varepsilon)^4 = 2$, e allora $(1+\varepsilon)$ ha necessariamente ordine 8, quindi è un generatore e il gruppo è ciclico.
- In $\mathbb{F} = \frac{\mathbb{Z}_3[x]}{(x^2-2)}$ ogni classe è rappresentata da $\overline{a+bx}$, essendo $a+bx$ il resto della divisione di qualsiasi polinomio per x^2-2. Basta verificare che la somma e il prodotto tra classi sono gli stessi definiti più sopra da:

$$(a+\varepsilon b) + (c+\varepsilon d) = (a+c) + \varepsilon(b+d) \tag{71}$$

$$(a+\varepsilon b)(c+\varepsilon d) = (ac+2bd) + \varepsilon(ad+bc) \tag{72}$$

Per la somma è ovvio, per il prodotto si ha:

$$\left(\overline{a+bx}\right)\left(\overline{c+dx}\right) = \overline{(a+bx)(c+dx)} = \overline{ac + (ad+bc)x + bdx^2} \tag{73}$$

ma essendo:

$$ac + (ad+bc)x + bdx^2 = ac + 2bd + x(ad+bc) + bd\left(x^2-2\right) \tag{74}$$

si ottiene il risultato voluto:

$$\left(\overline{a+bx}\right)\left(\overline{c+dx}\right) = \overline{ac + 2bd + x(ad+bc)} \tag{75}$$

Considerato il campo $\frac{\mathbb{Z}_2[x]}{(x^3+x+1)} = Z_2[\alpha]$ con $\alpha^3 + \alpha + 1 = 0$

- Trovare $q(x) \in \mathbb{Z}_2[x]$, il polinomio minimo di $1 + \alpha^2$
- Verificare che α è un elemento primitivo.

Soluzione:

- Sia $\beta \in \mathbb{Z}_2[\alpha]$. $\mathbb{Z}_2[\alpha]$ è uno spazio vettoriale di dimensione 3 su $\mathbb{Z}_2$, i 4 elementi $\{1, \beta, \beta^2, \beta^3\}$ sono quindi dipendenti e quindi esistono 4 elementi c_i **non tutti nulli** di $\mathbb{Z}_2[\alpha]$ tali che:
$$c_0 + c_1\beta + c_2\beta^2 + c_3\beta^3 = 0 \tag{76}$$
Essendo $\beta = 1 + \alpha^2$, e $\alpha^3 + \alpha + 1 = 0$, si ha:
$$\begin{aligned}\left(1+\alpha^2\right)^2 &= 1 + \alpha + \alpha^2\\ \left(1+\alpha^2\right)^3 &= \alpha + \alpha^2\end{aligned}$$
Si ha quindi:
$$c_0 + c_1\left(1+\alpha^2\right) + c_2\left(1+\alpha+\alpha^2\right) + c_3\left(\alpha+\alpha^2\right) = 0$$
ovvero:
$$\begin{aligned}c_0 + c_1 + c_2 &= 0\\ c_2 + c_3 &= 0\\ c_1 + c_2 + c_3 &= 0\end{aligned}$$
E quindi, essendo la soluzione da trovare in $\mathbb{Z}_2$:
$$\begin{aligned}c_1 &= 0\\ c_0 = c_2 &= c_3 = 1\end{aligned}$$
Il polinomio cercato è quindi: $1 + x^2 + x^3$.
- $\mathbb{Z}_2[\alpha]$ e $\mathbb{Z}_2[\beta]$ sono ambedue spazi vettoriali su $\mathbb{Z}_2$ di dimensione 3 e campi con 8 elementi.
- In $\mathbb{Z}_2[\alpha]$, α è primitivo:
$$\begin{aligned}\alpha^3 &= \alpha + 1\\ \alpha^4 &= \alpha^2 + \alpha\\ \alpha^7 &= (\alpha+1)\left(\alpha^2+\alpha\right) = 1\end{aligned}$$
In $\mathbb{Z}_2[\beta]$, β è primitivo:

$$\beta^3 = \beta^2 + 1$$
$$\beta^4 = 1 + \beta + \beta^2$$
$$\beta^7 = \left(1 + \beta + \beta^2\right)\left(\beta^2 + 1\right) = 1$$

Osservazione 6.1 *Gli elementi di un campo di* 8 *elementi sono allora* $\{a + b\alpha + c\alpha^2\}$ *con* $a, b, c \in \mathbb{Z}_2$, *e con* $\alpha^3 + \alpha + 1 = 0$; α *è elemento primitivo (quindi di ordine* 7*) e le sue* 8 *potenze distinte sono gli elementi* $\neq 0$ *del campo che si presenta anche come il campo di spezzamento di* $x^8 - x \in \mathbb{Z}_2[x]$

$$x^8 - x = x(x-1)(x-\alpha)(x-\alpha^2)(x-\alpha^3)(x-\alpha^4)(x-\alpha^5)(x-\alpha^6)$$

Sia $Z_{11}[x]$ **l'anello dei polinomi in** x **a coefficienti in** Z_{11}.

- Mostrare che i due polinomi

$$p(x) = x^2 + 1$$
$$q(x) = x^2 + x + 4$$

  sono irriducibili.

- Costruire un isomorfismo tra $\frac{\mathbb{Z}_{11}[x]}{(p(x))}$ e $\frac{\mathbb{Z}_{11}[x]}{(q(x))}$

Soluzione:

- Per l'irriducibilità, essendo i due polinomi di secondo grado, basterebbe provare che non hanno soluzioni in $\mathbb{Z}_{11}$ sostituendo nei polinomi tutti gli elementi di $\mathbb{Z}_{11}$. E' però più utile, qui e in molti altri casi, usare un risultato sui residui quadratici che ora ricordiamo. In $\mathbb{Z}_p^*$ (p primo) se l'equazione $x^2 = b \neq 0$ ha soluzioni allora $b^{\frac{p-1}{2}} = 1$, e viceversa. In tale caso, le soluzioni sono due. Infatti Il teorema di Fermat ci dice che $\forall x \neq 0 \bmod(p)$:

$$x^{p-1} = 1$$

  Se esiste x tale che $x^2 = b$, si ottiene che deve essere:

$$b^{\frac{p-1}{2}} = x^{p-1} = 1$$

  vale anche il viceversa: assumiamo

$$b^{\frac{p-1}{2}} = 1$$

  Sia ora y un elemento primitivo di $\mathbb{Z}_p^*$. Allora esiste una potenza i per cui $b = y^i$. In particolare abbiamo $y^{i\frac{p-1}{2}} = 1$. Il teorema di Fermat assicura che $p-1$ (che è l'ordine di y perchè y è primitivo) deve dividere $i\frac{p-1}{2}$ e quindi i deve essere pari. Ponendo allora $x = y^{\frac{i}{2}}$abbiamo $x^2 = b$.

- Nel nostro caso, per il polinomio x^2+1 abbiamo: $(-1)^5 = -1$ e quindi non ci sono radici, nel caso invece del polinomio x^2+x+4, il discriminante dell'equazione è $1-16 = -15 = 7$ e $(7)^5 \bmod 11 = 10 = -1$ e quindi ancora non ci possono essere soluzioni.

- I due campi hanno lo stesso numero di elementi (121), e cercare elementi primitivi è molto noioso, è quindi molto meglio ragionare così: siano t e s, rispettivamente, una soluzione formale di $p(x)$ e $q(x)$:

$$t^2 = -1 = 10$$
$$s^2 + s = -4 = 7$$

Cerchiamo una funzione

$$f : \mathbb{Z}_{11}[t] \to \mathbb{Z}_{11}[s]$$

tale che $[f(t)]^2 = -1$. Ponendo

$$f(t) = x + sy$$

e svolgendo i semplici calcoli, si trova

$$f(t) = 6 + s$$

Infatti

$$(6+s)^2 = 36 + 12s + s^2 = 3 + s + s^2 = 3 - 4 = -1$$

Allora:

$$f(a+bt) = a + (6+s)\, b$$

è l'isomorfismo cercato.

Trovare il campo di spezzamento del polinomio $x^4 + 2x^3 + 2x + 2 \in \mathbb{Z}_3[x]$
Soluzione:
il polinomio non ha radici in $\mathbb{Z}_3$ e quindi dobbiamo vedere se si spezza in fattori irriducibili di grado 2. Si pone quindi:

$$x^4 + 2x^3 + 2x + 2 = \left(x^2 + ax + b\right)\left(x^2 + cx + d\right)$$

Un semplice calcolo mostra che si ricava:

$$x^4 + 2x^3 + 2x + 2 = \left(x^2 + 1\right)\left(x^2 + 2x + 2\right)$$

Consideriamo il polinomio irriducibile (x^2+1), e sia α una sua radice. L'altra radice è chiaramente $-\alpha = 2\alpha$. Il campo di spezzamento di x^2+1 è

$$\frac{\mathbb{Z}_3[x]}{(x^2+1)} = \mathbb{F}_9 = \left\{0, 1, 1+1 = 2 = \alpha^2, \alpha, 2\alpha, 1+\alpha, 2+\alpha, 1+2\alpha, 2+2\alpha\right\}$$

In questo campo si ha:

$$\left(x^2+1\right) = (x-\alpha)(x-2\alpha) = (x+2\alpha)(x+\alpha)$$

Consideriamo ora il polinomio (x^2+2x+2). Cerchiamo le sue radici complesse formali: (la formula risolutiva delle equazioni di secondo grado si può applicare perchè non siamo in caratteristica 2 e quindi si può dividere per 2)

$$x = -1 \pm i$$

In $\mathbb{F}_9$, α si comporta come i ($\alpha^2 = 2 = -1$) e quindi in $\mathbb{F}_9$ anche il polinomio (x^2+2x+2) ha le sue due radici $-1 \pm \alpha$. Abbiamo allora:

$$\left(x^2+2x+2\right) = (x-(-1+\alpha))\,(x-(-1-\alpha)) = (x+1+2\alpha)\,(x+1+\alpha)$$

In definitiva abbiamo che $\mathbb{F}_9$ è il campo di spezzamento di x^4+2x^3+2x+2 :

$$x^4+2x^3+2x+2 = (x+2\alpha)\,(x+\alpha)\,(x+1+2\alpha)\,(x+1+\alpha)$$

Trovare il campo di spezzamento del polinomio $x^5+x^4+1 \in \mathbb{Z}_2[x]$
Soluzione:

il polinomio non ha radici in $\mathbb{Z}_2$ e quindi dobbiamo vedere se si spezza in fattori irriducibili di grado 2 e 3 : Si pone quindi:

$$x^5+x^4+1 = \left(x^2+ax+b\right)\left(x^3+cx^2+dx+e\right)$$

Un semplice calcolo mostra che si ricava:

$$x^5+x^4+1 = \left(x^2+x+1\right)\left(x^3+x+1\right)$$

Consideriamo il polinomio irriducibile (x^2+x+1), e sia α una sua radice. L'altra radice è $1+\alpha$. Il campo di spezzamento di x^2+x+1 è

$$\frac{\mathbb{Z}_2[x]}{(x^2+x+1)} = \mathbb{F}_4 = \{0, 1, \alpha, 1+\alpha\}$$

In questo campo si ha:

$$\left(x^2+x+1\right) = (x+\alpha)\,(x+1+\alpha)$$

Ora però il polinomio (x^3+x+1) è irriducibile su $\mathbb{F}_4$ perchè non ha radici in $\mathbb{F}_4$ e quindi si deve costruire il campo $\mathbb{F}_4[\beta]$ dove β è una radice di (x^3+x+1) :

$$\mathbb{F}_4[\beta] = \left\{a+b\beta+c\beta^2 \text{ con } a,b,c \in \mathbb{F}_4 \text{ e } \beta^3+\beta+1=0\right\}$$

Questo campo, isomorfo a $\mathbb{F}_{64}$ è il campo di spezzamento cercato infatti contiene tutte le radici di (x^3+x+1).

Troviamole: $(x^3+x+1) = (x-\beta)\,(x^2+\beta x+\beta^2+1)$ e le radici del polinomio $(x^2+\beta x+\beta^2+1)$ si possono trovare osservando che per una equazione di secondo grado monica, anche in caratteristica 2 dove non si può applicare la formula risolutiva, la somma delle radici è il coefficiente di x e il prodotto delle radici è il termine noto.

Una radice è β^2, infatti $\beta^4+\beta^3+\beta^2+1=0$ e l'altra è $\beta+\beta^2$.

Infatti:

$$(x+\beta)\left(x+\beta^2\right)\left(x+\beta+\beta^2\right) = x^3+\beta^4+\beta^5+x\beta^2+x\beta^3+x\beta^4 = x^3+x+1$$

Allora si trova la scomposizione in fattori lineari:

$$x^5+x^4+1 = (x+\alpha)(x+1+\alpha)(x+\beta)\left(x+\beta^2\right)\left(x+\beta+\beta^2\right)$$

Un polinomio irriducibile in $F_p[x]$ di grado m si dice primitivo se ha una radice che è un elemento primitivo di F_{p^m}

1. - Dimostrare che $x^4+x^3+1 \in \mathbb{Z}_2[x]$ è irriducibile in $\mathbb{Z}_2[x]$ e primitivo.
   - Dimostrare che invece $x^4+x^3+x^2+x+1 \in \mathbb{Z}_2[x]$ è irriducibile in $\mathbb{Z}_2[x]$ ma non è primitivo.

Soluzione: $x^4+x^3+1 \in \mathbb{Z}_2[x]$ è irriducibile perchè non ha radici in $\mathbb{Z}_2$ e non si può neanche scrivere come prodotto di due polinomi di secondo grado. Infatti:

$$x^4+x^3+1 = \left(x^2+ax+1\right)\left(x^2+bx+1\right) = ax+bx+2x^2+x^4+ax^3+bx^3+abx^2+1 \quad (77)$$

che è impossibile perchè, grado per grado, si avrebbe:

$$a+b=1 \quad (78)$$
$$ab=0 \quad (79)$$
$$a+b=0 \quad (80)$$

Analogamente si procede per dimostrare l'irriducibilità dell'altro polinomio.

Sia ora α una radice di x^4+x^3+1, si ha allora $\alpha^4+\alpha^3+1=0$. L'ordine di α non può essere 3, infatti $\alpha^3 \neq 1$ e non può essere nemmeno 5, infatti si ottiene: $\alpha^5+\alpha^4+\alpha=0$ e quindi $\alpha^5 \neq 1$. Allora l'ordine deve essere 15 e quindi α è primitivo per il campo di 16 elementi.

Invece $x^4+x^3+x^2+x+1 \in \mathbb{Z}_2[x]$ non è primitivo, infatti se β è una radice si ottiene subito:

$$\beta^4+\beta^3+\beta^2+\beta+1=0 \Rightarrow \beta^5 = \beta^4+\beta^3+\beta^2+\beta = 1 \quad (81)$$