Algebra Domini Euclidei (Unimib)

24 gennaio 2022

wikitolearn
collaborative textbooks

This book is the result of a collaborative effort of a community of people like you, who believe that knowledge only grows if shared.
We are waiting for you!

Get in touch with the rest of the team by visiting http://join.wikitolearn.org

Capitolo 1

Domini Euclidei

1.1 Dominio euclideo

1.1.1 Definizione

Definizione (323 Dominio euclideo e norma euclidea)

Un dominio D non ridotto a zero si dice *euclideo* se esiste una funzione $\nu\colon D^* \to \mathbb{Z}_0$ ($\mathbb{Z}_0$ = interi maggiori o uguali a zero) tale che

1. $\forall a, b \in D$ con $a, b \neq 0$, $\nu(a) \leq \nu(ab)$.
2. $\forall a, b \in D$ con $b \neq 0$, esistono $q, r \in D$ tali che sia $a = bq + r$ ove $r = 0_D$ oppure se $r \neq 0$, $\nu(r) < \nu(b)$.

ν viene chiamata norma euclidea.

1.1.2 Esempi di domini euclidei

Esempio (324)

Il dominio degli interi è euclideo e la norma è $|\dots|$. Infatti la condizione $0 < r < |b|$ imposta nell'algoritmo della divisione equivale alla condizione 2 di ν , inoltre il fatto che $|a| \leq |ab|$ garantisce la condizione 1.

Esempio (325)

Se F è un campo, il dominio dei polinomi a coefficienti nel campo è euclideo. Si assume come norma, per ogni polinomio non nullo, il grado. La condizione 2 è soddisfatta perché nella divisione si richiede che $gr(r(x)) < gr(b(x))$. Viene soddisfatta anche la condizione 1, perché il grado del prodotto è la somma dei gradi e quindi $gr(a) < gr(a) + gr(b)$ cioè $\nu(a) < \nu(ab)$.

1.1.3 Interi di Gauss

Definizione (326 Interi di Gauss)

Si chiamano interi di Gauss i numeri complessi a coordinate intere nel piano di Argand-Gauss, cioè quelli della forma $x + iy$ con $x, y \in \mathbb{Z}$.

In questo modo gli interi di Gauss formano un sottoanello dei complessi. Si definisce per ogni intero di Gauss il quadrato del modulo, cioè $\nu(x + iy) = x^2 + y^2$.

Proposizione (327)

Gli interi di Gauss formano un dominio euclideo.

Dimostrazione

Siccome $\nu(a, b) = \nu(a) * \nu(b)$ con a, b interi di Gauss, la condizione 1 della definizione di dominio euclideo è soddisfatta.

L'inverso di un numero complesso è il coniugato diviso per la norma, cioè $(x - iy)/(x^2 + y^2)$. L'inverso di un intero di Gauss in generale non è un intero, ma un razionale.

Per quanto riguarda la condizione 2, presi due interi $a, b \in G$ con $a \neq b$, devo trovare $p, q \in G$ tali che $a = qb+r$ con $\nu(r) < \nu(b)$. Considero il numero complesso $ab^{-1} = \psi + iz$. $\psi, z \in \mathbb{Q}$. Posso sicuramente trovare due interi $m, n \in \mathbb{Z}$ tali che $|\psi - m| \leq 1/2$ e $|z - n| \leq 1/2$. Chiamiamo $\psi - m = \varepsilon$ e $z - n = \eta$. Scriviamo allora

$$a = b*a*b^{-1} = b*(\psi+i*z) = b*[(m+\varepsilon)+i(n+\eta)] = b*(m+in)+b(\varepsilon+i\eta) =$$

$m + in$ è un intero di Gauss e lo chiamo q , b è un intero di Gauss.

Invece $r = b * (\varepsilon + i\eta)$ è tale che $r = a - b * q$, quindi è anch'esso un intero di Gauss. Calcolo la norma di r .

$$\nu(r) = |b|^2 * (\varepsilon^2 + \eta^2)$$
$$\varepsilon = \psi - m \leq 1/2$$
$$\varepsilon^2 \leq 1/4$$
$$\eta = z - n \leq 1/2$$
$$\eta^2 \leq 1/4$$
$$\nu(R) \leq |b|^2 * 1/2 \leq 1/2 * \nu(b)$$

allora $\nu(R) \leq \nu(b)$ se $R \neq 0$. Ho trovato due interi di Gauss q, r che soddisfano la condizione 2 .

Si possono determinare gli elementi unitari e gli elementi primi del dominio degli interi di Gauss ($\pm 1, \pm i$). In questo dominio i primi coincidono con gli irriducibili.

1.1.4 Caratterizzazione dei domini euclidei

Si può provare che ogni dominio euclideo è un dominio a ideali principali.

Teorema (328)

Ogni dominio euclideo d è un dominio a ideali principali (PID), cioè ogni suo ideale è principale.

Dimostrazione

Sia $I \neq 0$ un ideale del dominio euclideo D . Sia b un elemento di I che abbia norma minima fra gli elementi non nulli dell'ideale I (per il principio del buon ordinamento l'insieme delle norme ha un minimo). Sia $a \in I$. Siccome D è euclideo, esistono $q, r \in D$ tali che $a = bq + r$ tali che $r = 0$ o $\nu(r) < \nu(b)$. Ora, $R = a - bq$. $a, b, q \in I$, e I è un ideale chiuso rispetto al prodotto e alla differenza, quindi $a - bq = R \in I$. La scelta minimale di b forza $r = 0$ (infatti, $r \in I$, b ha norma minima tra gli elementi di I e $0 < \nu(r) < \nu(b)$). Si ha che $a = qb$. Allora $a \in I$ e $I \in (b)$, ma $b \in I$, questo implica che $(b) \in I$. Segue $I = (b)$, cioè ogni ideale del dominio è principale.

In base a questo teorema l'anello dei polinomi $F[x]$ su un campo F è un dominio a ideali principali (è euclideo).

Per la proprietà del trasporto, se F è un dominio, $F[x]$ è un dominio. Però non è vero che se F è a ideali principali, allora $F[x]$ è a ideali principali.

Questo è un esempio di dominio a ideali non principali con coefficienti su un dominio a ideali principali.

Esempio (329)

Considero $\mathbb{Z}$, insieme dei polinomi a coefficienti interi. Consideriamo l'insieme di tutti i polinomi in $\mathbb{Z}$ con termine noto pari. Esso è un ideale J , infatti la differenza di due polinomi con termine noto pari è ancora un polinomio con termine noto pari. Lo stesso vale per il prodotto. Quindi è un ideale, ma non è principale. Se fosse principale, sarebbe generato da un elemento con termine noto pari. Siccome in questo ideale c'è anche $f(z) = 2$, esso può essere l'unico generatore. Ma questo significa che qualsiasi polinomio si ottiene moltiplicando per 2 un polinomio a coefficienti interi, ma in questo modo si ottengono polinomi con tutti i coefficienti pari. I polinomi con termine noto pari e coefficienti dispari non rientrano. Isolando in un polinomio il termine noto, la parte restante è un polinomio divisibile per x . J è un ideale generabile da due elementi x e 2 ma non è principale.

1.1.5 Condizione di primarità

Se p è irriducibile, le uniche possibili fattorizzazioni per p sono $p = u * u^{-1}p$ con u unitario.

Abbiamo provato che in ogni dominio, p primo implica p irriducibile. In ogni dominio a ideali principali vale anche il viceversa.

Proposizione (330)

Se D è un PID, allora ogni elemento irriducibile in D è primo (condizione di primarità).

Osservazione (331)

Questo significa che in un PID le nozioni di primo e irriducibile sono equivalenti.

Dimostrazione

Sia p un elemento di D irriducibile. Supponiamo che $p \mid ab$, $a, b \in D$, ma $p \nmid a$. Proviamo che allora $p \mid b$.

Siccome p è irriducibile, allora non esiste alcun ideale J di D tale che $(p) \subset J \subset D$ (dipende dall'ipotesi che D è un dominio a ideali principali, in cui se p è irriducibile, (p) è massimale).

Siccome $p \nmid a$, allora $a \notin (p)$ e $(p)+(a)$ è l'intero D perché il generatore dell'ideale è unitario ($M.C.D.(a, p) = 1_D$). Segue che $1_D = xp + ya$ per opportuni $x, y \in D$. Moltiplicando per b entrambi i membri dell'uguaglianza, segue $b = 1_D * b = xpb + yab = xpb + ypc = p(xb + yc)$ cioè $p \mid b$. (l'ultimo passaggio vale perché $p \mid ab$).

In un dominio a ideali principali primo e irriducibile hanno lo stesso significato.

1.1.6 osservazioni

Osservazione (332 Proprietà fondamentale dell'aritmetica)

Ogni intero si può decomporre in modo unico in fattori primi.

Equivalentemente, ogni polinomio si può decomporre in modo unico come prodotto di fattori irriducibili.

Preso un dominio a fattorizzazione unica come $\mathbb{Z}$, la proprietà di fattorizzazione si eredita al corrispondente anello polinomiale. Essendo $\mathbb{Z}$ a fattorizzazione unica, anche $\mathbb{Z}$ è a fattorizzazione unica.

Osservazione (333)

In un generico anello commutativo A se I è un ideale di A , l'anello quoziente A/I è un dominio, se e solo se I è un ideale primo. A/I è un campo se e solo se I è massimale. In particolare, supponiamo che D non ridotto al solo zero sia un dominio a ideali principali. Allora un ideale non nullo generato da un elemento p è primo se e solo se p è primo. (p) è massimale se e solo se p è irriducibile. In forza della proposizione precedente, poiché in un dominio a ideali principali primo e irriducibile sono condizioni equivalenti, possiamo concludere che nell'insieme degli ideali non nulli, gli ideali primi coincidono con gli ideali massimali.

1.2 Polinomi

1.2.1 Polinomio irriducibile

Definizione (334 Polinomio irriducibile)

Sia F un campo e $F[x]$ il corrispondente anello dei polinomi in x a coefficienti in F . Esso è un dominio a ideali principali. Un polinomio $p(x) \in F[x]$ si dice *irriducibile* (= primo) se il grado di $p(x)$ è maggiore di zero (le costanti sono escluse) e gli unici fattori di $p(x)$ in $F[x]$ sono i polinomi di grado zero, cioè le costanti non nulle (elementi unitari) e i polinomi della forma $k * p(x)$ con k costante non nulla. In altre parole, le uniche fattorizzazioni ammesse da $p(x)$ sono quelle della forma $p(x) = k * k^{-1} * p(x)$,

1.2.2 Rappresentazione costante degli elementi del quoziente

Sia ora $(0) \neq I[x]$ un ideale dell'anello $F[x]$. Esso è principale e sarà generato da un polinomio, cioè $I[x] = (g(x))$. Possiamo supporre anche che il grado n del generatore $g(x)$ sia positivo per evitare il caso banale in cui $I[x] = F[x]$ (infatti una costante genera tutto $F[x]$), ovvero $\frac{F[x]}{I[[x]} = 0$.

Allora vale il seguente

Teorema (335 Rappresentazione standard degli elementi dell'anello quoziente $\frac{F[x]}{I[x]}$)

Nelle ipotesi precedenti, ogni elemento dell'anello quoziente $F[x]/I[x]$ (cioè ogni laterale di $I[x]$) contiene uno e un solo polinomio $R(x)$ di grado inferiore al grado n del generatore di $I[x]$. In altre parole: ogni laterale dell'ideale $(G(x))$ in $F[x]$ si può rappresentare in un unico modo nella forma: $[g(x)] + r(x)$ ove il grado di $r(x)$ è minore di n .

Dimostrazione

Sia $(g(x)) + a(x)$ un generico elemento di $\frac{F[x]}{I[x]}$. Dividiamo $a(x)$ per $g(x)$:

$$a(x) = q(x) * g(x) + r(x)$$

(vale sempre in un dominio euclideo)

e $gr(r(x)) < n$.

D'altronde posso riscrivere

$$r(x) = a(x) - q(x) * g(x)$$

siccome $g(x) \in I[x]$, allora $q(x) * g(x) \in I[x]$. Allora $r(x)$ e $a(x)$ differiscono per un elemento dell'ideale, quindi $r(x) \in (g(x)) + a(x)$. Ho provato che in ogni

laterale è possibile trovare un polinomio con grado inferiore a quello di $g(x)$. Mostriamo che tale polinomio è unico.

Supponiamo che $(g(x))+r(x)$ contenga un altro polinomio $r_1(x)$ con $gr(r_1(x)) < n$. Allora la differenza $r(x) - r_1(x) \in (g(x))$, allora è prodotto di $g(x)$ per un altro elemento dell'anello e quindi ha grado maggiore di n . L'unica possibilità per cui la differenza sta dentro è che $r_1(x) - r(x) = 0$, cioè $r(x) = r_1(x)$. Questo unico polinomio di cui il teorema garantisce l'esistenza può essere scelto come rappresentante standard.

Corollario (336)

Sia F un campo finito di ordine q . Supponiamo $gr(g(x)) = n$. Allora l'anello quoziente $F[x]/(g(x))$ è un anello finito e il numero dei suoi elementi è q^n .

Dimostrazione

La cardinalità di $F[x]/g(x)$ per la rappresentazione standard è uguale al numero dei polinomi a coefficienti in F di grado minore di n . Preso un polinomio $f(x)$ si può scrivere come $f(x) = a_{n-1} * x^{n-1} + a_1 * x_1 + a_0$. Ci sono n coefficienti e q scelte per ogni coefficiente, cioè q^n scelte in totale.

Se $g(x)$ è irriducibile, l'anello è un campo. Siccome ogni elemento del campo è rappresentabile da un polinomio di grado minore di n , identificando le costanti con gli elementi di F ottengo un campo più grande di F che lo contiene.

Preso un campo finito $\frac{\mathbb{Z}}{p\mathbb{Z}}$ con p primo. Allora per ogni $n > 0$ esiste per ogni possibile n posso costruire un campo di ordine q^n .

Caratteristica: periodo additivo dell'unità. In un campo finito la caratteristica è finita, e quindi dev'essere un numero primo. In realtà tutti gli elementi hanno periodo finito p . Ogni campo finito ha per ordine una potenza di p .

Per ogni numero primo p e per ogni n maggiore di 0 esiste un campo finito di ordine p^n . Campi finiti dello stesso ordine sono isomorfi tra di loro.

1.2.3 Ampliamento di campi

Consideriamo l'anello dei polinomi $F[x]$ a coefficienti in un campo F . Consideriamo l'ideale $I[x]$ generato da $g(x)$ con grado n positivo. Allora per il teorema di rappresentazione gli elementi dell'anello quoziente possono essere rappresentati come $I[x] + r(x)$ con $r(x)$ polinomio di grado minore di n , che è unico. Di conseguenza, se F è un campo finito di ordine q , allora l'anello quoziente ha cardinalità q^n .

Considero l'applicazione $J\colon F \to \frac{F[x]}{(g(x))}$ tale che per ogni $\lambda \in F$, $J(\lambda) = (g(x))+\lambda$. J è un monomorfismo di anelli. Infatti, se ho due scalari λ, μ , si ha come immagine il laterale $(g(x)) + \lambda + \mu$ e lo stesso vale per il prodotto. Il morfismo è iniettivo, perché $\lambda \in \ker F$ se e solo se $\lambda \in (g(x))$. Ma questa possibilità si verifica solo se $\lambda = 0$, perché ogni polinomio in $(g(x))$ ha grado maggiore di n . Possiamo identificare tramite J un sottoanello.

Allora possiamo pensare F contenuto nell'anello quoziente $\frac{F[x]}{(g(x))}$. In particolare, se $g(x)$ è irriducibile in $F[x]$ ovvero se l'anello quoziente è un campo, possiamo

considerare $E = \frac{F[x]}{(g(x))}$ come un ampliamento del campo F .

Quindi, preso un campo arbitrario e considerato un polinomio irriducibile con grado maggiore di 1, si può considerare un campo in relazione con quel polinomio.

1.2.4 Esempio 1: campo reale

Se F è il campo reale, allora $g(x) = x^2 + 1$ è irriducibile in $F[x]$. Infatti, se fosse riducibile, dovrebbe avere dei fattori propri, cioè si potrebbe scrivere $x^2 + 1 = (x-a) * (x-b) = x^2 - (a+b)x + ab$. Ponendo i coefficienti del polinomio trovato uguali a quelli di $x^2 + 1$ si ha $ab = 1, a + b = 0$, cioè $a = -b$ e $b^2 = -1$.

Allora l'anello quoziente generato da $x^2 + 1$ è un campo e sappiamo che ogni elemento di E è rappresentabile in modo unico nella forma:

$$(x^2 + 1) + (a_0 + a_1 * x)\, a_0, a_1 \in \mathbb{R}$$

(cioè ideale generato dal polinomio più un polinomio di grado minore)

Quindi il campo E che estende i reali è un campo con polinomi con grado ≤ 1 . Per quanto riguarda la somma, se consideriamo E come l'insieme dei polinomi $a_0 + a_1 x$, $a_0, a_1 \in \mathbb{R}$, la somma di due laterali ha come rappresentante la somma dei polinomi rappresentanti.

Se identifichiamo E come l'insieme dei polinomi, il prodotto è calcolato modulo $x^2 + 1$. Cioè,

$$(a_0 + a_1 x)(b_0 + b_1 x) = (x^2 + 1)(a_1 b_1) + (a_0 b_0 - a_1 b_1) + (a_0 b_1 + a_1 b_0) * x$$

Bisogna considerare come prodotto il resto della divisione del prodotto ordinario per $x^2 + 1$.

Prodotto ordinario:

$$(a_1 x + a_0)(b_1 x + b_0) = a_1 b_1 x^2 + (b_0 a_1 + a_0 b_1)x + a_0 b_0$$

Divisione per $x^2 + 1$:

$$q(x) = a_1 b_1$$

$$r(x) = (a_0 b_1 + a_1 b_0)x + a_0 b_0 - a_1 b_1 \text{ polinomio di grado 1}$$

E' chiaro allora che l'applicazione che al generico elemento $a_0 + a_1 x$ di E associa il numero complesso $a_0 + a_1 i$ realizza un isomorfismo fra il campo E e il campo complesso $\mathbb{C}$.

Il quoziente di un anello rispetto a un ideale è un campo se e solo se l'ideale è massimale, cioè se è generato da un irriducibile.

1.2.5 Esempio 2: campo digitale

Considero il campo delle classi di resti modulo 2 $\mathbb{Z}/2\mathbb{Z}$ che ha come elementi le classi di resti $[0], [1]$. Considerando lo stesso polinomio x^2+1 esso è uguale a $(x+1)^2 = x^2+2x+1 = x^2+[0]x+1$ quindi questo è un polinomio riducibile in $\frac{\mathbb{Z}}{2\mathbb{Z}}[x]$ e quindi l'anello quoziente non è un campo e non è un dominio, ma ha divisori dello zero. Infatti, preso $x+1$ nel quoziente, si ha che $(x+1)(x+1) = x^2+1$ che è lo zero del quoziente.

Preso $g(x) = x^2+x+1$, questo polinomio è irriducibile, altrimenti si potrebbe scrivere:

$$x^2+x+1 = (x-a)(x-b) = x^2-(a+b)x+ab$$

cioè

$$a+b=1 \quad ab=1 \quad a=1-b \quad b*(1-b)=1 \quad b-b^2=1 \quad b^2-b+1=0$$

e l'ultima condizione non è possibile perché $\Delta < 0$. Il quoziente $\frac{\mathbb{Z}/2\mathbb{Z}\quad[x]}{(x^2+x+1)}$ è un campo di ordine $4 = q^n = 2^2$.

Sia $F = \frac{\mathbb{Z}}{3\mathbb{Z}}[x]$, $g(x) = x^2+1$ è irriducibile in $\frac{\mathbb{Z}}{3\mathbb{Z}}[x]$, E è un campo che ha elementi $3^2 = 9$ elementi. E' possibile scrivere le tavola di composizione rispetto alla somma e al prodotto:

Elementi di $\frac{\mathbb{Z}/2\mathbb{Z}\quad[x]}{(x^2+1)}$: $0, 1, x, x+1$.

Tavole del prodotto modulo x^2+1 :

$*$	0	1	x	$x+1$
0	0	0	0	0
1	0	1	x	$x+1$
x	0	x	$-1=1$	$x-1=x+1$
$x+1$	0	$x+1$	$x+1$	0

(si vede che ci sono divisori dello zero, non è un campo).

Tavole del prodotto modulo x^2+x+1 :

	0	1	x	$x+1$
0	0	0	0	0
1	0	1	x	$x+1$
x	0	x	$-x-1=x+1$	1
$x+1$	0	$x+1$	1	x

1.3 Domini a fattorizzazione unica

1.3.1 Proprietà importanti

La classe dei PID è contenuta nella classe degli UFD (domini a fattorizzazione unica).

La proprietà di essere a fattorizzazione unica si trasporta dal dominio alla sua estensione polinomiale.

Valgono le seguenti osservazioni:

Osservazione (337)

1. Se D è un dominio e scrivo $a \sim b$ se e solo se esiste $u \in U$ tale che $a = ub$, cioè a differisce da b per un elemento

unitario, allora $\sim$ è una relazione di equivalenza.

Dim. E' riflessiva infatti $a = 1_D * a$ con $1_D \in U$, è simmetrica infatti $ua = b$ implica $a = u^{-1}b$ con $u^{-1} \in U$ e transitiva, infatti se $a = u_1 b$ e $b = u_2 c$ allora $a = u_1 u_2 c$.

1. Se $u_1, u_2 \in U$, essi sono associati, cioè $u_1 \sim u_2$, perché u_1 differisce per un elemento unitario da u_2 , infatti $u_1 * u_2^{-1}$ è ancora unitario.
2. Se $u \in U$ è unitario e $u_1 \sim u$, allora u_1 è unitario. Cioè gli elementi unitari formano un'unica classe di equivalenza

rispetto alla relazione $\sim$.

1. Se $a \sim b$ e b è irriducibile in D , allora anche a è irriducibile in D .

Moltiplicando un elemento irriducibile per un unitario ottengo ancora un irriducibile.

1. Se $a \in D$ e $a \mid u \in U$ allora $a \in U$ (gli unici divisori di elementi unitari sono unitari).

1.3.2 Definizione di UFD

Definizione (338 Dominio a fattorizzazione unica)

Sia D non ridotto a zero un dominio. D si dice *dominio a fattorizzazione unica* se preso un qualsiasi elemento $a \in D$ dove $0 \neq a$ e a non unitario, si può scrivere a come prodotto di fattori irriducibili, cioè $a = p_1 * \cdots * p_r$ dove i p_i sono irriducibili in D . Se $a = q_1 * \cdots * q_s$ e q_j sono irriducibili in D , allora $r = s$ cioè le due fattorizzazioni hanno lo stesso numero di elementi (*lunghezza di* a) e a meno di un eventuale riordinamento dei q_j , $q_j \sim p_j$ per ogni $j = 1, r$. (negli interi differisce per il segno, nei polinomi per una costante)

1.3.3 Relazione tra PID e UFD

Proposizione (339)

Ogni dominio a ideali principali è anche un UFD .

Dimostrazione

Proviamo che se D è un PID , vale la condizione $*$: non si trovano in D sequenze infinite di elementi del tipo $a_1, a_2, a_i, a_{i+1}, \dots$ ove per ogni i a_{i+1} è un fattore proprio del precedente. (ovvero, in ogni sequenza tale che $a_{i+1} \mid a_i$ esiste N tale che $a_N \sim a_{N+1} \sim a_{N+2}$ (la sequenza diventa stazionaria).

$*$ è equivalente alla $**$: D non contiene alcuna catena propriamente ascendente infinita di ideali principali del tipo $(a_1) \subset (a_2) \subset (a_i) \subset (a_{i+1})$ (infatti in un PID, $a_1 \mid a_2 \longrightarrow (a_2) \subset (a_1)$).

Supponendo D a ideali principali dimostriamo la condizione $**$: Chiamiamo $I = \bigcup_{i \in I}\{(a_i)\}$. Osserviamo che I è un ideale (e siccome siamo in un PID è un ideale principale). L'unione insiemistica di ideali con una catena ascendente di inclusioni è undeale, perché è uguale al più grosso di questi ideali uniti.

Sia $I = (d)$, allora esiste n tale che $d \in (a_n)$ e segue quindi $I = (d) \subseteq (a_n)$. Inoltre, per ogni $M \geq N$, segue che $(a_n) \subseteq I \subseteq (a_m)$, ma siccome I è l'unione, non esistono ideali più grossi quindi $(a_m) = (a_n)$ (la catena è stazionaria).

Esistenza di una fattorizzazione: Sia $0 \neq a$ un elemento non unitario di D . Allora mostriamo che a si può esprimere come prodotto di irriducibili. Se a è irriducibile, non ho niente da provare.

In caso contrario, se a è riducibile, allora a ha dei fattori propri e posso scrivere $a = a_1 b_1$ con a_1 fattore proprio. Allora si possono verificare due possibilità:

1. a_1 è irriducibile.
2. a_1 è riducibile, e quindi posso scrivere $a_1 = a_2 * p_2$ con a_2 fattore proprio.

Itero il ragionamento su a_2 . Si forma una sequenza $a, a_1, a_2, \dots$ che in forza della proprietà $*$ deve terminare dopo un numero finito di passi con un fattore irriducibile di a . Diciamo a_n irriducibile in D e lo chiamiamo p_1 . Posto $p_1 = a_n$, si ha che $a = p_1 * a'$, perché ho scoperto che a ha un fattore irriducibile. Allora se consideriamo a' , se $a' \in U$, allora a è irriducibile (alterando un irriducibile per un fattore unitario è ancora irriducibile). Altrimenti, se a' non è unitario, posso ripetere il ragionamento fatto su a . E posso scrivere $a' = p_2 * a''$ con p_2 irriducibile. Iterando la procedura, si ottiene una sequenza fatta da $a, a', a'', \dots, a^{(i)}$ e così via, ove $a^{(i)}$ divide $a^{(i-1)}$ propriamente. Inoltre, $a^{(i-1)} = ab^{(i)}$ con $b^{(i)}$ irriducibile. Per la condizione $*$ tale sequenza deve terminare, con un elemento irriducibile. Allora pongo l'ultimo elemento $a^{(r-1)} = p_r$, e segue che $a = p_1 * a' = p_1 p_2 * a'' = p_1 * p_2 * p_r$. Questo prova che ogni elemento del dominio ha una fattorizzazione in termini irriducibili.

Unicità: useremo implicitamente la nozione di fattori primi, se p è primo e divide il prodotto di un certo numero di fattori, divide almeno uno di questi (si prova per induzione o usando l'associatività). Supponiamo di avere due fattorizzazioni: supponiamo di avere $a = p_1 p_2 * p_r = q_1 q_2 q_s$ dove p_i e q_j sono irriducibili.

Proviamo per induzione su r che in realtà le due fattorizzazioni coincidono. Se $r = 1$, allora $a = p_1$. a è irriducibile, allora non può essere fattorizzato in più di un fattore riducibile. Allora se $a = p_1$, anche $p_1 = q_1$ e $s = 1$.

Supponiamo $r > 1$ e presa la prima fattorizzazione, p_1 è irriducibile e p_1 divide il prodotto $q_1 q_2 q_r = a$. Allora deve dividere almeno uno dei fattori, cioè $p_1 \mid q_j$ per qualche j (p_1 è anche primo). Ma anche q_j è irriducibile e ammette solo fattori banali. Allora $p_1 \sim q_j$. Eventualmente riordinando possiamo supporre $j = 1$, cioè $p_1 \mid q$ e $q_1 = u_1 p_1$ con $u_1 \in U$. Allora

$$a = p_1 p_2 p_r = q_1 q_2 q_s = u_1 * p_1 q_2 q_s$$

valgono le leggi di cancellazione, quindi semplifico per p_1 e ottengo:

$$p_2 \dots p_r = u_1 \dots q_2' \dots q_s$$

Ci sono due fattorizzazioni irriducibili di un elemento b e la lunghezza della prima fattorizzazione è $r - 1$. Quindi per induzione su r questa fattorizzazione è unica. Allora $r - 1 = s - 1$ e $r = s$, inoltre eventualmente riordinando $p_i \sim q_i$ per ogni $i \geq 2$.

Esempio (340)

$$d = \mathbb{Z}(\sqrt{-5}) = \{z \in \mathbb{C}\, t.c.\, z = a + \sqrt{5} * ib \quad a, b \in \mathbb{Z}\}$$

Si considera una norma euclidea. Se prendo $r = a + b * \sqrt{-5}$, la norma $n(r) = a^2 + 5b^2$.

Calcolo gli elementi unitari del dominio. Siccome la norma è moltiplicativa, presi due elementi r, s in D si ha

$$n(rs) = n(r) * n(s)$$

allora considero r unitario in D tale che $rs = 1_D$. Le norme sono interi non negativi, allora se $rs = 1$, con r unitario e s il suo inverso, si ha

$$n(rs) = n(r) * n(s) = n(1) = 1$$

e necessariamente $n(r) = n(s) = 1$.

Questo implica che $r = \pm 1$. Questi sono gli unici elementi unitari in D .

In questo anello prendo il numero 9 . Posso fattorizzarlo come $3 * 3$ oppure come $(2 + \sqrt{-5})(2 - \sqrt{-5})$. Ho due fattorizzazioni in elementi di D si verifica che sia 3 che $2 \pm \sqrt{-5}$ sono irriducibili.

Gli elementi irriducibili sono a due a due non associati. Quindi si hanno due fattorizzazioni distinte dell'elemento 9 in elementi irriducibili. Questi elementi sono irriducibili ma non primi. In questo dominio ci sono irriducibili che non sono primi. Questo allora non è un UFD e non è un dominio a ideali principali.

1.4 Radici di un polinomio

1.4.1 Anello delle funzioni

Sia X un insieme non vuoto. Allora possiamo considerare l'insieme Y^X di tutte le applicazioni da X a Y . Sia A un anello. Allora con A^X si indica l'insieme di tutte le applicazioni da X ad A . Allora possiamo definire una somma e un prodotto.

1. Per ogni $f, g \in A^X$, la somma $f + g$ è tale che $\forall x \in X$, $(f + g)(x) = f(x) + g(x)$ (la somma delle immagini si può definire

perché le immagini sono elementi di A).

1. Analogamente il prodotto $(fg)(x)$ ha come risultato il prodotto delle immagini $f(x) * g(x) \in A$.

Si dà così a A^X una struttura di anello: l'anello delle funzioni da X ad A .

Nel caso particolare in cui $X = \{1, 2, n\}$, allora l'anello delle funzioni da X ad A è isomorfo ad A^n . A è un anello commutativo e indichiamo con $A[x]$ l'anello dei polinomi a coefficienti in A .

1.4.2 Funzione polinomiale

Definizione (341 Funzione polinomiale)

Se $f(x) = a_n * x^n + a_{n-1} * x^{n-1} + a_1 * x + a_0$ definiamo una funzione associata $F\colon A \to A$ tale che $\forall \alpha \in A$, $F(\alpha) = a_n * \alpha^n + a_{n-1} * \alpha^{n-1} + \cdots + a_1 * \alpha + a_0$ (si sostituisce all'indeterminata x uno scalare $\alpha \in A$). Questa funzione F si dice *funzione polinomiale* associata al polinomio f . Per abuso di linguaggio, scriveremo $f(\alpha)$ invece di $F(\alpha)$.

Lemma (342)

Consideriamo l'applicazione $\phi\colon A[x] \to A^A$ definita ponendo, per ogni $f(x) \in A[x]$:

$$\phi(f(x)) = F(x)$$

è l'applicazione che a ogni polinomio associa la sua applicazione polinomiale. ϕ è un morfismo di anelli tra l'anello dei polinomi e l'anello delle funzioni polinomiali. (ϕ associa alla somma e al prodotto di polinomi rispettivamente la somma e il prodotto delle funzioni polinomiali).

Nella dimostrazione si tiene conto del fatto che x e α commutano con tutte le costanti.

Dimostrazione

Siano $a(x) = a_n * x^n + a_1 * x + a_0$ e $b(x) = b_b * x^n + b_1 * x + b_0$ due polinomi, allora:

$$\phi(a(x)+b(x)) = \phi(a_n*x^n+\cdots+a_1*x+a_0+b_n*x^n+\cdots+b_1*x+b_0) = a_n*\alpha^n+b_n*\alpha^n+$$

$$+\cdots+a_1*\alpha+b_1*\alpha+a_0+b_0 = (a_n+b_n)x^n+\cdots+(a_1+b_1)*\alpha+a_0+b_0 = (a+b)(\alpha)$$

In particolare, per il lemma preso un polinomio $f(x) = a(x) * b(x)$, allora calcolando $f(\alpha)$ si ha $f(\alpha) = a(\alpha) * b(\alpha)$ (il valore della funzione polinomiale su α è uguale al valore del prodotto delle immagini).

1.4.3 Omomorfismo di valutazione

Supponiamo di avere una qualsiasi estensione di anelli $A \subset B$. Allora possiamo considerare l'anello $A[x]$ che è un sottoanello di $B[x]$. Allora per ogni $f(x) \in A[x]$ e per ogni $b \in B$, possiamo considerare l'elemento $f(b)$ che è un elemento di B , cioè valutare $f(x) \in B$.

Definizione (343 Omomorfismo di valutazione)

La mappa B_b da $A[x] \to B$ definita ponendo $B_b(f(x)) = f(b)$ per ogni $f(x) \in A[x]$, è un morfismo di anelli e si chiama *omomorfismo di valutazione*.

Osservazione (344)

Considerando l'omomorfismo ϕ , esso in generale non è iniettivo. Preso un anello commutativo generico non è necessariamente vero che due polinomi distinti hanno funzioni polinomiali distinte.

Se A è finito, l'anello delle funzioni di A in sé è finito, mentre il dominio di ϕ è infinito perché i polinomi possono avere tutti i gradi possibili, quindi ϕ va da un insieme infinito a uno finito e non può essere iniettivo. Ad esempio, se A è finito l'anello A^A è finito e quindi il nucleo non può essere ridotto a zero.

Esempio (345)

Supponiamo che A sia $\frac{\mathbb{Z}}{p\mathbb{Z}}$, il campo delle classi di resti modulo p con p primo. Allora tutte le classi hanno inverso rispetto al prodotto, cioè $U = (\mathbb{Z}/p\mathbb{Z})^*$, cioè gli elementi unitari sono tutte le classi di resti $[a]_p$ diverse dalla classe $[0]$, cioè con a coprimo con p . Per il teorema di Lagrange presa una qualsiasi classe $[a]_p$ diversa dalla classe $[0]$, $[a]_p^{p-1} = 1_A$ (in termini di congruenze, se p è un primo arbitrario e a un intero coprimo con p , allora $a^{p-1} \equiv 1 \mod p$) (teorema di Fermat).

Possiamo concludere che comunque si scelga un elemento $[a]_p$ nel campo $\frac{\mathbb{Z}}{p\mathbb{Z}}$, allora se considero $([a]_p)^p - [a]_p = [a]_p * \{([a]_p)^{p-1} - 1_P\} = 0_p$. Infatti se $[a]_p = 0$ il primo termine del prodotto è nullo e quindi il tutto è uguale a 0. Se invece $[ap] \neq 0$, allora $[a]_p^{p-1} \equiv 1 \mod p$ e $1_A - 1_A = 0$ e anche in questo caso il prodotto si annulla.

Ciò significa che la funzione polinomiale associata al polinomio di grado p $x^p - x$ è la funzione identicamente nulla, cioè coincide con la funzione polinomiale associata al polinomio nullo.

1.4.4 Radice di un polinomio

Definizione (346 Radice di un polinomio)

Sia $A \subset B$ un'estensione di anelli e sia α un elemento di B . Se P_α è l'omomorfismo di valutazione in α , allora se $P_\alpha(f(x)) = 0$, diremo che α è una *radice* o *zero* del polinomio $f(x) \in B$.

1.4.5 Teorema di Ruffini

Sia ora $A = F$ un campo. Allora vale il seguente teorema.

Teorema (347)

Sia F un campo e $f(x)$ un polinomio a coefficienti in F . Allora α è radice di $f(x)$ se e solo se $x - \alpha \mid f(x)$.

Dimostrazione

Supponiamo che $x - \alpha$ divida $f(x)$, cioè $f(x) = (x - \alpha) * q(x)$. Allora se valuto in α $f(x)$, si ha $f(\alpha) = (\alpha - \alpha) * q(\alpha) = 0$. Allora $f(\alpha) = 0$ ovvero α è radice di $f(x)$.

Viceversa, supponiamo che $f(\alpha) = 0$. Allora possiamo dividere $f(x)$ per $x - \alpha$ e otteniamo:

$$f(x) = (x - \alpha) * q(x) + r(x)$$

dove $r(x)$ ha grado minore di $gr(x - \alpha) < 1$.

Allora

$$0 = f(\alpha) = (\alpha - \alpha) * q(\alpha) + r(\alpha)$$

per il morfismo ϕ .

Siccome $\alpha - \alpha = 0$ rimane $r(\alpha)$. Allora $r(x) = r$ è una costante ed è un elemento di F . Allora valutando r in α , ottengo sempre r . Quindi si ha $0 = f(\alpha) = r$ e $0 = r$, cioè il resto è nullo, quindi $f(x) = (x - \alpha) * q(x)$, cioè se x è una radice, $x - \alpha$ divide $f(x)$.

1.4.6 Relazione tra radici e riducibilità

Corollario (348)

Se un polinomio $f(x) \in F[x]$ ha grado maggiore di 1 e ha una radice $\alpha \in F$, allora è riducibile su F (infatti ha almeno il fattore $x - \alpha$).

Osservazione (349)

Un polinomio di grado 1 $a_1 * x + a_0$ in $f(x)$ con $a_1 \neq 0$ ha un'unica radice $-a_1^{-1} * a_0 \in F$ ed è irriducibile.

Corollario (350)

Se $f(x)$ è un polinomio a coefficienti in F di grado 2 o 3 è riducibile se e solo se ammette una radice in F .

Dimostrazione

Un polinomio riducibile di grado 2 è fattorizzabile nel prodotto di due polinomi di grado 1 . Un polinomio di grado 3 invece viene fattorizzato in tre polinomi di grado 1 o un polinomio di grado 2 e uno di grado 1 . Il fattore di grado 1 che compare si può scrivere come $a_1 * x + a_0$. Allora $-a^{-1} * a_0$ è una radice.

Osservazione (351)

Un polinomio $f(x) \in F[x]$ può essere riducibile in $F[x]$ ma non ammettere alcuna radice in $F[x]$.

Esempio (352)

Il polinomio a coefficienti reali

$$f(x) = x^4 + 3x^2 + 2 = (x^2 + 1)(x^2 + 2)$$

E' un polinomio riducibile di grado 4 , ma i suoi fattori di grado 2 sono irriducibili e quindi il polinomio non ha radici.

1.4.7 Molteplicità di una radice

Definizione (353 Molteplicità di una radice e radice semplice)

Sia $f(x) \in F[x]$ un polinomio e sia α una costante. Diremo che α è radice di $f(x)$ di *molteplicità* r con $r \geq 1$ se $(x - \alpha)^r \mid f(x)$ ma $(x - \alpha)^{r+1} \nmid f(x)$. Se $r = 1$ α si dice *radice semplice*.

Questa definizione vale in forza del teorema di Ruffini e del teorema di fattorizzazione unica.

1.4.8 Esempi

Esempio (354)

In $\mathbb{Q}$ x^4-2x^2+1 è fattorizzabile come $(x+1)^2*(x-1)^2$. A meno di fattori unitari, questa fattorizzazione completa del polinomio è unica. Allora il polinomio ha esattamente 2 radici (altrimenti comparirebbe un altro fattore) con molteplicità 2 .

Esempio (355)

$$p(x) = x^5 - x^4 - 7x^3 + 11x^2 - 8x + 12 = (x-2)^2 * (x+3) * (x^2+1)$$

Nella fattorizzazione c'è un fattore irriducibile sui razionali e tre fattori lineari. Le radici sono 2 con molteplicità 2 e -3 con molteplicità 1 .

Esempio (356)

Nel campo delle classi di resto modulo 2 , che chiamo $\frac{\mathbb{Z}}{2\mathbb{Z}}$,

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

ha come radice solo 1 con molteplicità 4 .

$$p(x) = x^3 + x + 1$$

non ha radici in $\frac{\mathbb{Z}}{2\mathbb{Z}}$ infatti

$$p(0) = 1\, p(1) = 3$$

e essendo un polinomio di grado 3 è anche irriducibile in $\mathbb{Z}$.

Esempio (357)

Considero il campo delle classi di resto modulo p con p numero primo arbitrario fissato. Considero il polinomio:

$$p(x) = x^p - x$$

esso ha come radici semplici tutti gli elementi del campo $\frac{\mathbb{Z}}{p\mathbb{Z}}$ e quindi è fattorizzabile nella forma:

$$x^p - x = \prod_{s=0}^{p-1} (x-s)$$

.

1.4.9 Conseguenza del teorema di fattorizzazione unica

Teorema (358)

Sia $f(x)$ un polinomio non nullo a coefficienti in F con grado n . Allora la somma delle molteplicità delle eventuali radici di $f(x)$ in F non supera n .

Dimostrazione

Se $n = 0$, $f(x) = a_0$ con $a_0 \neq 0$. Questo polinomio vale a_0 su qualsiasi elemento di F e quindi non ha radici.

Supponiamo $n > 0$. Allora vale il teorema di fattorizzazione unica, allora $f(x)$ è decomponibile in modo unico in fattori irriducibili in $F[x]$. Se nessuno di questi fattori ha grado 1 , allora per il teorema di Ruffini $f(x)$ non ha radici in F e il teorema è provato. In caso contrario, sarà $* = f(x) = k * (x - \alpha_1)^{r_1} * \cdots * (x - \alpha_t)^{r_t} * g_1(x) * g_s(x)$ con $k \in F^*$ costante non nulla, $\alpha_1, \dots \alpha_t$ elementi distinti di F e $g_1(x), \dots g_s(x)$ sono eventuali polinomi (irriducibili) in $F[x]$ di grado maggiore di 1 . Per l'unicità della fattorizzazione $*$ è chiaro che $\alpha_1, \dots, \alpha_t$ sono radici di $F[x]$ in F di molteplicità esattamente r_1, r_t . E' anche evidente che $f(x)$ non ha altre radici in F . Infatti, se $p(x)$ avesse radice β , $x - \beta$ dovrebbe comparire tra gli altri fattori. Se β fosse radice di $f(x)$ con $\beta \neq \alpha_1, \alpha_t$, avremmo

$$f(\beta) = (\beta - \alpha_1)^{r_1} * \cdots * (\beta - \alpha_t)^r_t * g_1(\beta) * g_s(\beta)$$

e questo è assurdo, perché allora tutti questi fattori sono diversi da 0, i g_i non sono uguali a 0 perché sono irriducibili. Ho un prodotto di elementi diversi da 0 che non può essere uguale a zero in un dominio privo di divisori dello zero, quindi β non è una radice.

Osservazione (359)

In base all'ultimo passo della dimostrazione si capisce che il teorema precedente è falso per anelli $A[x]$ ove A non è un campo (o un dominio).

Esempio (360 Controesempio)

In $\frac{\mathbb{Z}}{6\mathbb{Z}}$ $2, 3$ sono divisori dello zero. Il polinomio a coefficienti in questo anello:

$$p(x) = x^2 - 5x$$

è di grado 2 . Si può valutarlo in tutti gli elementi e si scopre che ha $0, 2, 3, 5$ come radici. Il polinomio ha grado 2 ma ha quattro radici distinte.

1.4.10 Caso particolare: iniettività del morfismo phi

Corollario (361)

Sia F un campo (dominio) infinito. Allora l'omomorfismo di anelli $\phi\colon F[x] \to F^F$ cioè quello che a ogni polinomio associa la sua funzione polinomiale, è iniettivo.

Dimostrazione

Supponiamo che $f(x)$ sia un polinomio che sta nel nucleo di ϕ . Allora la sua funzione polinomiale f è la funzione identicamente nulla, cioè per ogni $\alpha \in F$, $f(\alpha) = 0$. Allora se F è infinito, $f(x)$ ha infinite radici (tutti gli elementi di F). Per il teorema precedente, $f(x)$ deve essere il polinomio nullo, altrimenti la

somma delle molteplicità delle radici supera il suo grado. Quindi se F è infinito, è lecito identificare i polinomi con le funzioni polinomiali.

Anticipazione: preso un qualsiasi dominio, si può passare al suo campo delle frazioni, cioè si può immergere un dominio di integrità in un campo.

1.4.11 Principio d'identità dei polinomi

Corollario (362)

Siano $\alpha_0, \alpha_1, \ldots, \alpha_n$ $n+1$ elementi distinti del campo F . Allora valgono le seguenti asserzioni:

1. Siano $a(x), b(x)$ polinomi in $F[x]$ di grado $\leq n$, tali che si abbia $a(\alpha_i) = b(\alpha_i)$ per $i = 0, n$. Allora i due polinomi coincidono, cioè $a(x) = b(x)$.
2. Siano $\beta_0, \ldots \beta_n$ $n+1$ elementi non necessariamente distinti nel campo F . Allora esiste ed è unico un polinomio $l(x)$ a coefficienti in F con grado $\leq n$ tale che $l(\alpha_i) = \beta_i$.

Dimostrazione

Nel punto 1 , sia $f(x) = a(x) - b(x)$ allora $gr(f(x)) \leq n$ ma $f(x)$ ammette le $n+1$ radici $\alpha_0, \alpha_1, \ldots, \alpha_n$. Questo contraddice il teorema sulla molteplicità delle radici, e il polinomio $f(x)$ con le $n+1$ radici distinte è il polinomio nullo, cioè $a(x) - b(x) = 0$ e $a(x) = b(x)$.

Per il punto 2 , in base al punto 1 esiste al più un polinomio di $F[x]$ soddisfacente le condizioni richieste. Infatti se ne esistessero due, $l_1(x)$ e $l_2(x)$ che assumono lo stesso valore sugli α_i , la loro differenza $l_1(\alpha_i) - l_2(\alpha_i) = \beta_i - \beta_i = 0$ e la differenza avrebbe ancora $n+1$ radici distinte ed è quindi il polinomio nullo, cioè $l_1(x) = l_2(x)$.

Per quanto riguarda l'esistenza di tale polinomio, considero il polinomio

$$l(x) = \sum_{r=0}^{n} (\beta_r * \prod_{j \neq r} \frac{x - \alpha_j}{\alpha_r - \alpha_j})$$

.

(La frazione equivale a moltiplicare $(x - \alpha_j)$ per $(\alpha_r - \alpha_j)^{-1}$).

Ciascuno di questi prodotti ha grado minore di n , perché è prodotto di n fattori lineari (si esclude il termine con $r = j$). Sommando i termini il grado è sicuramente minore o uguale di n e $l(\alpha_i) = \beta_i$.

Infatti, sostituendo x con α_i , se $i \neq r$ sarà $i = j$ per un certo j allora nel prodotto ci sarà un termine al numeratore della forma $\alpha_i - \alpha_j = 0$ e tutto il prodotto si annulla. Nell'unico termine del prodotto in cui $i = r$, numeratori e denominatori si semplificano a due a due e rimane β_i . L'unico termine che contribuisce alla sommatoria è $g(\alpha_i) = \beta_i$.

Un polinomio di questo tipo si chiama *interpolatore di Lagrange*.

1.4.12 Nozione di riducibilità

Supponiamo che il campo F ammetta un'estensione E , cioè un campo che lo contiene. Allora se considero l'anello dei polinomi a coefficienti in F , $F[x] \subset E[x]$. Allora considerato un polinomio $f(x)$ a coefficienti in F , eventuali fattori irriducibili $p(x) \in F[x]$ di un polinomio $f(x) \in F[x]$ di grado maggiore di 1 possono essere riducibili in $E[x]$, così che $f(x)$ può essere ulteriormente fattorizzato in $E[x]$. Quindi la nozione di riducibilità e irriducibilità è relativa al campo in cui si pensa il polinomio.

1.4.13 Chiusura algebrica

In effetti, è possibile dimostrare che assegnato un campo F arbitrario, si può sempre trovare un'estensione di F con le seguenti proprietà:

- ogni polinomio di $E[x]$ di grado positivo e a maggior ragione ogni polinomio di $F[x]$ di grado positivo è fattorizzabile in polinomi

di grado 1 (polinomi lineari).

- se $\bar{E}$ è un'estensione di F con la proprietà che ogni polinomio di grado positivo di $F[x]$ è fattorizzabile

in fattori lineari in $(\bar{E})[x]$ allora $\bar{E}$ contiene un sottocampo isomorfo a E .

Un campo E estensione di F con tale proprietà è unico a meno di isomorfismi e si dice *chiusura algebrica* di F . Se $F = E$, si dice che F è un campo *algebricamente chiuso*. In altre parole:

Definizione (363 Campo algebricamente chiuso)

Un campo F si dice algebricamente chiuso se valgono queste condizioni che sono tra loro equivalenti:

1. preso un qualsiasi polinomio $a(x) \in F[x]$ di grado $n > 0$ esso è fattorizzabile in esattamente n polinomi di grado 1 appartenenti a $F[x]$.
2. Equivalentemente, ogni polinomio $a(x) \in F[x]$ di grado positivo ammette almeno una radice in F .
3. la somma delle molteplicità delle radici di ogni polinomio $a(x) \in F[x]$ di grado n è esattamente uguale a n .

Le prime due condizioni sono equivalenti perché se un polinomio di grado n ammette una radice, allora è divisibile per $x - \alpha$ e si ha $p(x) = (x - \alpha) * q(x)$. Allora anche $q(x)$, se non è una costante, ha grado positivo e avrà anch'esso una radice allora $x - \alpha_2$ divide $q(x)$ e si va avanti così finché non si ottiene una costante e si ha $p(x) = (x - \alpha) * (x - \alpha_2) * \cdots * (x - \alpha_n)$.

1.4.14 Teorema fondamentale dell'algebra

Teorema (364 Teorema fondamentale dell'algebra)

Il campo complesso $\mathbb{C}$ è algebricamente chiuso ed è la chiusura algebrica del campo reale (a meno di isomorfismi la chiusura è unica).

Corollario (365)

Ogni polinomio $f(x)$ a coefficienti reali di grado positivo si decompone in $\mathbb{R}$ in polinomi irriducibili di grado minore o uguale di 2 .

Dimostrazione

Mostriamo che se α è radice di $f(x)$, anche $\bar{\alpha}$ è radice. Infatti se α è radice, $0 = f(\alpha)$.

$$a_n * \alpha^n + a_{n-1} * \alpha^{n-1} + a_1 * \alpha + a_0 = 0 = \bar{0} = a_n * \bar{\alpha}^n + a_{n-1} * \alpha^{n-1} + \cdots + a_1 * \bar{\alpha} + a_0$$

e si ottiene

$$a_n * \bar{\alpha}^n + \cdots + a_1 + \bar{\alpha} = 0$$

cioè $\bar{\alpha}$ è radice.

Immaginiamo che α sia complesso e non reale. Questo significa che $f(x)$ è divisibile per

$$(x - \alpha)(x - \bar{\alpha}) = x^2 - (\alpha + \bar{\alpha}) * x + \alpha * \bar{\alpha}$$

.

Allora siccome $\alpha + \bar{\alpha} \in \mathbb{R}$ e $\alpha * \bar{\alpha} \in \mathbb{R}$ ho un polinomio a coefficienti in $\mathbb{R}$.

1.4.15 Esempi: determinare polinomi irriducibili

In generale, preso un polinomio e un campo F ci si può chiedere se il polinomio ha radici, se è irriducibile e se è fattorizzabile in irriducibili.

Esempio (366)

Considero i polinomi a coefficienti complessi. Allora ogni polinomio si può decomporre in fattori lineari. I polinomi irriducibili in $\mathbb{C}$ sono tutti e soli i polinomi lineari di grado 1 della forma $a_1 * x + a_0$ (per il teorema fondamentale dell'algebra).

Esempio (367)

Nell'anello $\mathbb{R}$ i polinomi irriducibili in $\mathbb{R}$ sono i polinomi lineari e i polinomi di grado 2 della forma $a_2 * x^2 + a_1 * x + a_0$ in cui $\Delta = a_1^2 - 4a_2a_0$ è negativo nei reali.

Esempio (368)

Se considero il campo dei numeri razionali, non si può dire quali siano i polinomi irriducibili, ma si sa che sono infiniti e di ogni grado n possibile. Sia p un numero intero primo e per ogni $n > 0$ il polinomio

$$f(x) = x^n - p$$

è irriducibile sui razionali.

Questo si prova in generale mediante il *criterio di Eisenstein*.

Criterio di Eisenstein: sia $f(x) = a_n * x^n + a_{n-1} * x^{n-1} + a_1 * x + a_0$ un polinomio a coefficienti interi. Allora se esiste un primo p tale che $p \mid a_i$ per $i = 0, n-1$ ma $p \nmid a_n$ (a_n = coefficiente direttivo) e $p^2 \nmid a_0$, allora il polinomio $f(x)$ è irriducibile in $\mathbb{Q}(x)$.

L'esempio di prima soddisfa il criterio di Eisenstein: infatti il termine noto è $a_0 = p$ e non è divisibile per p^2 , il coefficiente direttivo è 1 e non è divisibile per p , tutti gli altri coefficienti sono zeri e sono divisibili per p .

Nella dimostrazione del criterio di Eisenstein si utilizza il *Lemma di Gauss*:se ho un polinomio su un campo, se raccolgo l' $M.C.D.$ tra i coefficienti ottengo un polinomio con coefficienti coprimi tra loro (primitivo). Il prodotto di due polinomi primitivi è ancora primitivo.

Il criterio di Eisenstein e il lemma di Gauss sono enunciati formalmente e dimostrati al termine del capitolo.

Esempio (369)

Supponiamo che $F = \frac{\mathbb{Z}}{p\mathbb{Z}}(x)$. Allora esistono polinomi irriducibili di ogni grado possibile $n > 0$.

1.4.16 Esempi: decomposizione in fattori irriducibili

Esempio (370)

Se considero $\mathbb{R}$ e $\mathbb{C}$ non esistono algoritmi generali per determinare né gli zeri né le regole per decomporre in fattori irriducibili un polinomio $f(x)$ (metodi di approssimazione degli zeri, metodi di analisi numerica).

Esempio (371)

In $\mathbb{Q}$, esiste un algoritmo generale classico che si deve a Kronecker per decomporre un polinomio in fattori irriducibili. Questo metodo usa gli interpolatori di Lagrange, ma non è efficiente.

Esempio (372)

In $\frac{\mathbb{Z}}{p\mathbb{Z}}[x]$ esistono algoritmi di fattorizzazione di un polinomio in irriducibili efficienti derivanti dall'*algoritmo Berlekamp* (1970) , che si basa su metodi di algebra

lineare. Si riconduce il problema della fattorizzazione alla risoluzione di sistemi lineari.

Criterio: Se ho un polinomio a coefficienti interi

$$a_n * x^n + a_{n-1} * x^{n-1} + \cdots + a_1 * x + a_0$$

una frazione r/s è radice per il polinomio se e solo se r divide il termine noto e s divide il coefficiente direttivo.

1.4.17 Riduzione modulo un primo

Se ho un polinomio a coefficienti interi di grado n , prendo un primo che non divide il coefficiente direttivo. Se ad ogni coefficiente associo la corrispondente classe modulo p , ottengo il polinomio nel campo $\mathbb{Z}/p\mathbb{Z}$. Se questo polinomio è irriducibile in quel campo, allora il polinomio originario è irriducibile sui razionali.

Esempio (373)

Considero ad esempio

$$p(x) = 10x^3 - 13x - 8$$

A questo polinomio non posso applicare il criterio di Eisenstein, perché non posso trovare un primo p che divide il termine noto. Però se scelgo $p = 3$ riduco i coefficienti del polinomio modulo 3 e ottengo:

$$p(x) = x^3 + 2x + 1$$

come polinomio a coefficienti nelle classi di resti modulo 3 . Questo polinomio non ha radici in $\frac{\mathbb{Z}}{3\mathbb{Z}}$, infatti:

$$p(0) = 1 \quad p(1) = 4 \equiv 1 \mod 3 \quad p(2) = 13 \equiv 1 \mod 3$$

e quindi non ha radici nemmeno nel campo dei razionali.

1.5 Immersione di un dominio in un campo

1.5.1 Teorema

Ci si può chiedere se un dominio si può considerare come sottoanello di un opportuno campo.

Teorema (374)

Sia D un dominio. Ogni dominio D si può immergere in (è isomorfo a un sottoanello di) un campo F . Esiste D' sottoanello di F e un monomorfismo $\eta\colon D \to F$ tale che $\eta(D) = D'$.

Dimostrazione

Cominciamo con il supporre che D sia già un sottoanello di un campo E . Consideriamo il sottocampo F di E generato da D , cioè F è l'intersezione di tutti i sottocampi di E contenenti D .

Dimostro che $F = \{ab^{-1} \in E : a, b \in D, b \neq 0\}$. b^{-1} è l'inverso di b in E .

La parentesi a destra è un sottoinsieme di F , inoltre contiene D perché contiene tutti gli elementi $a * (1_D)^{-1} = a \in D$.

Inoltre, l'insieme tra parentesi graffe è un sottocampo di E infatti:

- è chiuso ridpetto alla differenza, infatti

$$a * b^{-1} - c * d^{-1} = a * b^{-1} * d * d^{-1} - c * d^{-1} * b * b^{-1} = (ad - bc) * (db)^{-1}$$

e questo è ancora un elemento dell'insieme tra parentesi graffe.

- è un sottogruppo di E rispetto al prodotto, cioè soddisfa il criterio $a * b^{-1}$ in G con $a, b \in G$

Prendo $a * b^{-1} = a$ $c * d^{-1} = b$. Allora

$$[(ab^{-1}) * (cd^{-1})]^{-1} = ab^{-1} * dc^{-1} = ad * (cb)^{-1}$$

che appartiene ancora all'insieme.

Quindi l'insieme tra parentesi è un sottocampo di E che contiene D ed è contenuto nell'intersezione di tutti i campi che contengono D , quindi coincide con F .

Con questo teorema si può capire come creare un campo che contiene un anello e che sia minimale.

Consideriamo l'insieme

$$D \times D^* = \{(a, b) t.c. a, b \in D, b \neq 0\}$$

Su $D \times D^*$ definiamo una relazione $\sim$ che associa a due coppie (a, b) e (c, d) se e solo se $ad = bc$. Questa relazione è di equivalenza. Allora consideriamo l'insieme quoziente $\frac{D \times D^*}{\sim}$. Denotiamo con a/b la classe di equivalenza contenente la coppia (a, b) . Ogni coppia (a, b) si chiama frazione. a/b è per abuso di linguaggio la frazione individuata dalla coppia (a, b) .

Sia F l'insieme quoziente $\frac{D \times D^*}{\sim} = \{a/b\}$ (qui, come nel teorema precedente, $F = \{ab^{-1},\ a, b \in D\}$). Notiamo che la classe di equivalenza $[a/b]$ coincide con $[c/d]$ se e solo se $ad = bc$.

Sull'insieme quoziente definisco somma e prodotto.

- La somma $[a/b] + [c/d] = [(ad + bc)/(bd)]$. Si può verificare che questa operazione è ben definita, cioè che cambiando

rappresentanti per le classi di equivalenza si trova come somma la stessa frazione.

- Il prodotto $[a/b] * [c/d] = [\frac{ac}{bd}]$. Il prodotto è ben definito e commutativo.

Rispetto alla somma, il quoziente è un gruppo abeliano con 0 uguale alla classe $[0/1]$ che contiene tutte le coppie del tipo $(0, b)$. Rispetto al prodotto, F^* è un gruppo con unità. L'unità è la classe $[1/1]$. L'inverso di $[a/b]$ è la classe di b/a .

Valgono le proprietà distributive, cioè F è un campo.

Consideriamo l'applicazione $\eta\colon D \to F$ definita ponendo per ogni elemento $a \in D$, $\eta(a) = a/1$. Questa applicazione η conserva la somma e il prodotto, quindi $\eta(a + b) = (a + b)/1 = a/1 + b/1 = \eta(a) + \eta(b)$.

Similmente è conservato il prodotto:

$$\eta(a * b) = (ab)/1 = a/1 * b/1 = \eta(a) * \eta(b)$$
$$\eta(1_D) = 1_D/1_D = 1_F$$

Il nucleo è ridotto a 0 , perché preso un elemento a con immagine $a/1$, se questo elemento ha come immagine $0/1$ si ha $a * 1 = 0 * 1$ cioè $a = 0$.

Quindi il morfismo è iniettivo, $\eta(D)$ è isomorfo a D ed è un sottoanello di F .

1.5.2 Osservazioni

Osservazione (375)

Identificando ogni $a \in D$ con $\eta(a) = a/1$, si identifica D con $\eta(D)$ e pertanto si può considerare D come sottoanello di F .

Osservazione (376)

Notiamo che per ogni a/b possiamo scrivere $a/b = a/1 * 1/b = (a/1) * (b/1)^{-1}$ allora a/b si può considerare come prodotto in F di a per l'inverso di b . Quindi per le considerazioni iniziali D genera F .

Nessun sottocampo proprio di F può contenere D .

1.5.3 Campo delle frazioni

Definizione (377 Campo delle frazioni)

Diremo che F è il *campo delle frazioni* o campo dei quozienti del dominio D .

Ad esempio, se D è il dominio degli interi, si può costruire come campo delle frazioni il campo dei razionali.

Si può provare il seguente teorema:

Teorema (378)

Costruiamo F e D come sopra. Sia η_d un monomorfismo di D a un campo F' , cioè un'immersione di D in un campo F' . Allora η_d si può estendere in un unico modo a un monomorfismo η_f dal campo F a F' , cioè si può estendere η_d a un morfismo di campi.

In particolare, se F' è generato da $\eta_d(D)$ allora è isomorfo a F perché deve contenere F .

Dimostrazione

Si consideri la mappa η_f che preso un elemento di F $a/b = ab^{-1}$ associa $\eta_d(a) * \eta_d(b)^{-1}$ che va da F a F' ed è un monomorfismo. η_f estende η_d , cioè $\eta_f(a) = \eta_d(a)$. E' iniettiva, è unica. Ogni $\bar{\eta}_f$ che estende η_d è tale che l'immagine di un qualsiasi elemento di F è necessariamente la stessa di η_f .

1.6 Proprietà degli UFD

1.6.1 Massimo comun divisore

Per i domini a ideali principali presi due elementi esiste sempre un $M.C.D.$ tra i due e vale l'identità di Bézout. Si può provare l'esistenza di un $M.C.D.$ per una sequenza di n elementi. Se definiamo in modo ovvio l' $M.C.D.$ di una lista, esso si definisce come $M.C.D.[M.C.D.(a_1, a_2, \ldots, a_{n-1}), a_n]$ riconducendolo al caso dell' $M.C.D.$ tra due elementi. Infatti se esiste l' $M.C.D.$ tra due elementi, per l'ipotesi induttiva esiste per $n-1$ elementi, allora esiste anche l' $M.C.D.$ degli n elementi.

Lemma (379)

Supponiamo che D sia un UFD . Per ogni coppia di elementi a, b non nulli, esiste un $M.C.D.(a, b)$.

Dimostrazione

Siano a, b due elementi non nulli di D . Osserviamo che se uno dei due è unitario, allora c'è un $M.C.D.$.

Infatti $a \mid b$, perché ogni elemento unitario è divisore di qualsiasi elemento e se b è unitario, $M.C.D.(a, b) = b$.

Supponiamo che a, b non sono unitari, allora sono decomponibili in un unico modo come prodotti di irriducibili. Consideriamo una fattorizzazione di a in irriducibili. Nella fattorizzazione ci possono essere dei fattori a due a due associati, che chiamo $p_1, p_2, \ldots, p_n$. Raccogliendo eventualmente gli elementi unitari, abbiamo:

$$a = u * p_1^{e_1} * \cdots * p_r^{e_r}$$

dove i p_i non sono fra loro associati, ma sono a due a due non associati.

Possiamo scrivere

$$a = u * p_1^{e_1} * \cdots * p_t^{e_t}$$

$$b = u' * p_1^{f_1} * \cdots * p_t^{f_t}$$

con u, u' elementi unitari e con $e_i, f_i > 0$ per ogni $0 < i < t$.

Come basi compaiono gli stessi fattori irriducibili, se un fattore irriducibile di a non è fattore di b , allora comparirà con esponente 0 nella fattorizzazione di b .

Chiamiamo $h_i = \min(e_i, f_i)$. Chiamiamo $d = p_1^{h_1} * \cdots * p_t^{h_t}$. Allora $d \mid a$ e $d \mid b$. Se $c \in D$ e $c \mid a$ e $c \mid b$, per l'unicità di fattorizzazione c è un

sottoprodotto di a e di b , cioè

$$c = \bar{u} * p_1^{l_1} * \cdots * p_t^{l_t}$$

con $0 \leq l_i \leq e_i, f_i$ per ogni i . Allora siccome $h_i = \min(e_i, f_i)$ questi fattori compaiono in c con esponenti che non superano e_i, f_i allora $c \mid d$ e d è massimo comun divisore.

1.6.2 Relazione tra primi e irriducibili

Lemma (380)

Sia D un dominio a fattorizzazione unica. Allora se $p \in D$ è irriducibile, p è necessariamente primo.

Dimostrazione

Sia p irriducibile in D e si supponga che $p \mid ab$ con $a, b \neq 0$. Allora esiste $c \in D$ tale che $ab = pc$. a può essere unitario e se $a \in U$, allora a è invertibile. Se a ammette inverso a^{-1} si può scrivere $p \mid b$. Similmente se b è unitario, ragionando allo stesso modo, $p \mid a$.

Supponiamo dunque che a, b non siano elementi unitari, allora sono fattorizzabili in irriducibili. Sia $a = p_1 * p_2 * p_s$ e $b = q_1 * q_2 * q_t$ ove i p_i e i q_j sono irriducibili in D . Allora il prodotto $ab = p_1 * \cdots * p_s * q_1 * \cdots * q_t$. Siccome per ipotesi $p \mid ab$ e p è irriducibile, allora per l'unicità della fattorizzazione p è associato a uno dei p_i o dei q_j cioè differisce da loro per un elemento unitario. Allora se p è associato a p_i , si ha $p \mid a$. Se invece $p \sim q_i$ si ha $p \mid b$.

Consideriamo $D = \mathbb{Z}$ dominio a fattorizzazione unica e sia $f(x) \in P[x]$ un polinomio a coefficienti non nulli. Se $D = \mathbb{Z}$, allora $\mathbb{Z}$ ha ideali non principali, pur essendo a fattorizzazione unica, nonostante $\mathbb{Z}$ sia a ideali principali. Per questo era necessario estendere i due lemmi ai UFD .

1.6.3 Polinomio primitivo

Definizione (381 Polinomio primitivo)

Se $f(x)$ è un polinomio si può scrivere

$$f(x) = a_n * x^n + a_{n-1} * x^{n-1} + \cdots + a_1 * x + a_0$$

Sia $c = c_F$ un $M.C.D.$ dei coefficienti non nulli di $f(x)$. Allora c è definito a meno di elementi unitari di D . Se $0 \neq f(x) \in P[x]$ si dice *primitivo* se $c = 1$, cioè se i coefficienti sono a due a due coprimi.

Osservazione (382)

Se c è come sopra, per ogni coefficiente si può scrivere $a_i = c * a'_i$ per $0 < i < n$. Allora posso raccogliere c da ciascun coefficiente e scrivere

$$f(x) = c * [a'_n * x^n + \cdots + a'_1 * x + a'_0]$$

e gli a'_i sono a due a due coprimi. Se chiamo $f_1(x) = a'_n * x^n + \cdots + a'_1 * x + a'_0$ esso è primitivo in $D[x]$.

Raccogliendo il massimo comun divisore tra i coefficienti ottengo uno scalare per un polinomio primitivo.

Notiamo che se $f(x) = c_1 * f_2(x)$ con $c_1 \in D$ e $f_2(x)$ primitivo in $D[x]$, si ha che $c_1 = u * c$ e $f_1(x)$ è associato a $f_2(x)$. Infatti per ogni coefficiente si ha:

$$a_i = c * a'_i = c_1 * a''_i$$

Siccome i coefficienti sono a due a due coprimi, c_1 è anch'esso $M.C.D.$ tra gli a_i e si può scrivere $c_1 = u * c$ con u unitario.

Allora

$$f(x) = c_1 * f_2(x) = u * c_1 * f_1(x)$$

cioè semplificando per c_1 , $u * f_1(x) = f_2(x)$, e quindi $f_1(x)$ e $f_2(x)$ sono associati.

1.6.4 Lemmi importanti

Lemma (383)

Se prendiamo un polinomio non nullo $0 \neq f(x)$ a coefficienti in $F[x]$ dove F è il campo delle frazioni di D , allora si può scrivere

$$f(x) = \alpha * f_1(x)$$

con α scalare non nullo in F e $f_1(x)$ polinomio primitivo in $D[x]$. Una tale espressione è unica a meno di elementi unitari.

Dimostrazione

Sia $f(x) = \alpha_n * x_n + \cdots + \alpha_1 * x + \alpha_0$ con $\alpha_i \in F$ e supponiamo che $\alpha_n \neq 0$, cioè $gr(f(x)) = n$. Per ogni i , $\alpha_i = a_i * b_i^{-1}$ dove $a_i, b_i \in D$ e $b_i \neq 0$ (gli α_i sono frazioni). Poniamo $b = \prod_{i=0}^{n} b_i$.

Allora $b*f(x)$ appartiene a $D[x]$ e per le osservazioni precedenti possiamo scrivere $b*f(x) = c*f_1(x)$ ove $c \in D$ e $f_1(x)$ ha coefficienti in D ed è primitivo. Posto $\alpha = cb^{-1}$, si ha $f(x) = \alpha * f_1(x)$.

Per quanto riguarda l'unicità, supponiamo che $f(x) = \beta * f_2(x)$ don $\beta \in F$ e $f_2(x) \in D[x]$ ed è primitivo. Sia $\beta \in F$, $\beta = d*e^{-1}$ con $d, e \in D$ e $e \neq 0$. Allora posso scrivere $f(x) = c*b^{-1}*f_1(x) = d*e^{-1}*f_2(x)$ da cui,

moltiplicando per b ed e

$$c*e*f_1(x) = d*b*f_2(x)$$

Quest'uguaglianza è un'uguaglianza fra polinomi in $D[x]$. Per quanto visto sopra, $ce = ubd$ in D . Quindi $db = uce$ per un opportuno u unitario in D . Segue che $de^{-1} = u*cb^{-1}$ ovvero β differisce da α per un elemento unitario u . Infine segue ancora che $\alpha * f_1(x) = \beta * f_2(x) = \alpha * u * f_2(x)$, cioè semplificando per α , $f_1(x)$ differisce da $f_2(x)$ per un elemento unitario e la scrittura sopra è unica a meno di elementi unitari.

Corollario (384)

Siano $f(x), g(x) \in D[x]$ primitivi e associati in $F[x]$ (cioè differenti per un elemento unitario di F cioè una costante non nulla). Allora $f(x)$ e $g(x)$ sono associati in $D[x]$, cioè differiscono per un elemento unitario di D .

Dimostrazione

Prendiamo $f(x)$, $g(x)$ polinomi di $D[x]$ associati in $F[x]$, allora $f(x) = \alpha * g(x)$ con $0 \neq \alpha \in F$. Inoltre, $\alpha \sim 1_F = 1_D$, quindi $1_d * f(x) = \alpha * g(x)$, quindi per la parte sull'unicità del lemma 1, $f(x) \sim g(x)$ e $1_D \sim \alpha$, cioè i due polinomi sono associati in $D[x]$.

Lemma (385 Lemma di Gauss)

Il prodotto di due polinomi $f(x), g(x)$ primitivi in $D[x]$ è primitivo in $D[x]$.

Dimostrazione

Supponiamo per assurdo che $h(x) = g(x)*f(x)$ non sia primitivo in $D[x]$. Allora $M.C.D.$ tra i coefficienti di $h(x)$ non è unitario. Allora esiste $p \in D$ irriducibile tale che $p \mid h(x)$ ma $p \nmid f(x) \wedge p \nmid g(x)$ perché $M.C.D.$ tra i coefficienti di $f(x)$ e $g(x)$ è 1 .

Siccome in ogni UFD ogni irriducibile è primo, allora p è primo in D . Ciò equivale a dire che l'anello quoziente $\bar{D} = \frac{D}{(p)}$ è un dominio, cioè non ha divisori dello zero (questo vale perché (p) è primo). Se $\bar{D}$ è un dominio, anche $\bar{D}[x]$ è un dominio. Chiamiamo ora $\phi \colon D[x] \to \bar{D}[x]$ l'omomorfismo indotto dall'epimorfismo canonico $: D \to \bar{D}$, che ad ogni elemento $d \in D$ associa $d + (p)$.

Invece il morfismo ϕ associa a ogni polinomio $f(x) \in D[x]$ il polinomio $\bar{a}^n * x_n + \cdots + \bar{a} * x + a + (p)$ dove (p) è l'ideale principale generato da p .

Siccome questo è un morfismo di anelli, allora

$$\phi(f(x) * g(x)) = \phi(f(x)) * \phi(g(x))$$

ovvero se $\bar{f}(x)$ è il polinomio immagine, posso riscriverlo come $\phi(h(x)) = \bar{h}(x) = \bar{f}(x) * \bar{g}(x)$. Ma $h(x)$ è divisibile per p . Tutti i coefficienti di $h(x)$ sono divisibili per p , allora nel quoziente i coefficienti sono tutti uguali a 0, cioè $\bar{h}(x) = 0$. Siccome $p \nmid f(x)$ si ha $\bar{f}(x) \neq 0, \bar{g}(x) \neq 0$.

Ma questa è una contraddizione, perché in un dominio non ci sono divisori dello zero.

Lemma (386 Conseguenza del Lemma di Gauss)

Sia $f(x)$ un polinomio a coefficienti in D irriducibile in $D[x]$ e di grado positivo (siccome non siamo in un campo, una costante non unitaria può essere riducibile). Allora $f(x)$ è irriducibile anche in $F[x]$. (un polinomio irriducibile negli interi lo è anche nei razionali)

Dimostrazione

$f(x)$ è necessariamente primitivo in $D[x]$, perché in caso contrario avrebbe una fattorizzazione non banale in $D[x]$ della forma $f(x) = a * \bar{f}(x)$ con a non unitario in D e non nullo.

Supponiamo per assurdo che $f(x)$ sia riducibile in $F[x]$, allora $f(x) = a(x) * b(x)$ a coefficienti in F entrambi di grado positivo.

Per il lemma 1 sappiamo che $a(x) = \alpha * f_1(x)$ e $b(x) = \beta * f_2(x)$ con $f_1(x), f_2(x)$ primitivi in $D[x]$ e α, β elementi di F , necessariamente unitari perché ogni costante è unitaria in un campo.

Segue che posso scrivere $f(x) = a(x) * b(x) = (\alpha\beta) * f_1(x) * f_2(x)$ dove siccome $f_1(x), f_2(x)$ sono primitivi in $D[x]$, allora il prodotto è primitivo in $D[x]$ per il lemma 2.

Segue a sua volta che per il corollario al lemma 1, un polinomio primitivo in $D[x]$ è uguale a uno scalare in F per un polinomio primitivo in $D[x]$. I due elementi differiscono per un elemento unitario. Poiché $f_1(x), f_2(x)$ hanno grado ≥ 0 , allora ho una contraddizione rispetto all'ipotesi che $f(x)$ è irriducibile in $D[x]$ perché ho una fattorizzazione non banale. Ciò conferma l'irriducibilità di $f(x)$ in $F[x]$, perché l'assurdo non può valere.

1.6.5 Criterio di Eisenstein

Teorema (387 Criterio di Eisenstein)

Sia $f(x) = a_n * x^n + \cdots + a_1 * x + a_0$ un polinomio a coefficienti interi appartenente a $\mathbb{Z}$ di grado n positivo. Supponiamo che esista un primo $p \in \mathbb{Z}$ tale che $p \mid a_i$ per ogni $i = 0, n-1$, $p \nmid a_n$, $p^2 \nmid a_0$. Allora $f(x)$ è irriducibile in $\mathbb{Q}$.

Dimostrazione

Osserviamo che poiché $p \nmid a_n$, allora senza perdere generalità possiamo supporre che $f(x)$ sia primitivo in $\mathbb{Z}$. Se non lo fosse, semplificando per il massimo comun divisore dei coefficienti si ottiene ancora un polinomio primitivo.

Supponiamo che $f(x)$ sia riducibile in $\mathbb{Q}$. Allora per il lemma 3, $f(x)$ è riducibile in $\mathbb{Z}$, sia $f(x)$ fattorizzabile come $b(x) * c(x)$ ove per assurdo $b(x), c(x)$ sono polinomi di grado positivo a coefficienti interi.

Scrivendoli esplicitamente si ha

$$b(x) = b_m * x^m + \cdots + b_1 * x + b_0$$
$$c(x) = c_{n-m} * x^{n-m} + \cdots + c_1 * x + c_0$$

sono polinomi in $\mathbb{Z}$ di grado maggiore di zero.

Se $f(x) = b(x) * c(x)$ allora il termine noto è il prodotto dei termini noti.

$$a_0 = b_0 * c_0$$

Siccome per ipotesi p è primo e divide a_0 , allora o $p \mid b_0$ o $p \mid c_0$. Supponiamo ad esempio che $p \mid b_0$. Per ipotesi, $p^2 \nmid a_0$, cioè se $p \mid b_0$, $p \nmid c_0$.

Consideriamo l'epimorfismo $\phi\colon \mathbb{Z} \to \frac{\mathbb{Z}}{p\mathbb{Z}}[x]$ indotto dall'epimorfismo canonico $: \mathbb{Z} \to \mathbb{Z}/(p)$.

$$\phi(p(x) = [a_n] * x^n + \cdots + [a_1] * x + [a_0]$$

Allora si ha che $\phi(f(x))$ siccome p divide tutti i coefficienti in mezzo, rimane solo $[a_n] * x^n$ e siccome $p \nmid a_n$, $[a_n] \neq [0]$ e questo non è il polinomio nullo. D'altronde $\phi(c(x)) = [c_{n-m}]_p * x^{n-m} + \cdots + [c_1]_p * x + [c_0]_p$. Siccome ϕ è un morfismo, si ha

$$\phi(f(x)) = \phi(b(x) * c(x))$$

cioè $\phi(c(x))$ è un fattore di $\phi(f(x))$. Ciò implica che $\phi(c(x)) = [c_{n-m}]_p * x^{n-m}$. Allora in particolare $[c_0]_p = 0 \in \frac{\mathbb{Z}}{p\mathbb{Z}}$ ma questo è assurdo perché $p \nmid c_0$.

Possiamo concludere che ci sono polinomi irriducibili sui razionali per ogni possibile grado. Allora i polinomi $a_n * x^n + a_0$ è sempre irriducibile per ogni grado.

Esiste anche l'algoritmo di Kroneker che permette di fattorizzare gli irriducibili sui razionali.

Si può anche scegliere un primo opportuno che non divide il coefficiente direttivo del polinomio. Si riducono i coefficienti di $f(x)$ modulo p se il polinomio non è riducibile in $\frac{\mathbb{Z}}{p\mathbb{Z}}$ non lo è nemmeno in $\mathbb{Q}$.

Se D è un dominio, $D[x]$ è a ideali principali solo se D è un campo.

Capitolo 2

Fonti per testo e immagini; autori; licenze

2.1 Testo

- **Corso:Algebra Domini Euclidei (Unimib)/Domini Euclidei/Dominio euclideo** *Fonte:* https://it.wikitolearn.org/Corso%3AAlgebra_Domini_Euclidei_(Unimib)/Domini_Euclidei/Dominio_euclideo?oldid=48247 *Contributori:* Toma.luca95 e Mmontrasio
- **Corso:Algebra Domini Euclidei (Unimib)/Domini Euclidei/Polinomi** *Fonte:* https://it.wikitolearn.org/Corso%3AAlgebra_Domini_Euclidei_(Unimib)/Domini_Euclidei/Polinomi?oldid=48340 *Contributori:* Toma.luca95 e Mmontrasio
- **Corso:Algebra Domini Euclidei (Unimib)/Domini Euclidei/Domini a fattorizzazione unica** *Fonte:* https://it.wikitolearn.org/Corso%3AAlgebra_Domini_Euclidei_(Unimib)/Domini_Euclidei/Domini_a_fattorizzazione_unica?oldid=48042 *Contributori:* Toma.luca95 e Mmontrasio
- **Corso:Algebra Domini Euclidei (Unimib)/Domini Euclidei/Radici di un polinomio** *Fonte:* https://it.wikitolearn.org/Corso%3AAlgebra_Domini_Euclidei_(Unimib)/Domini_Euclidei/Radici_di_un_polinomio?oldid=48035 *Contributori:* Toma.luca95 e Mmontrasio
- **Corso:Algebra Domini Euclidei (Unimib)/Domini Euclidei/Immersione di un dominio in un campo** *Fonte:* https://it.wikitolearn.org/Corso%3AAlgebra_Domini_Euclidei_(Unimib)/Domini_Euclidei/Immersione_di_un_dominio_in_un_campo?oldid=48310 *Contributori:* Toma.luca95 e Mmontrasio
- **Corso:Algebra Domini Euclidei (Unimib)/Domini Euclidei/Proprietà degli UFD** *Fonte:* https://it.wikitolearn.org/Corso%3AAlgebra_Domini_Euclidei_(Unimib)/Domini_Euclidei/Propriet%C3%A0_degli_UFD?oldid=48353 *Contributori:* Toma.luca95 e Mmontrasio

2.2 Immagini

2.3 Licenza dell'opera