Corso di Algebra 1

A. Machì

a. a. 2006–2007

Dispensa 5

1 Interi di Gauss

Per un numero complesso $\alpha = a + bi$, si definisce la *norma* $N(\alpha)$, cioè il prodotto di α per il suo coniugato $a-bi$; si ha $N(\alpha) = (a+bi)(a-bi) = a^2+b^2$. Come somma di quadrati di due numeri reali, la norma non è mai negativa. La norma è moltiplicativa: $N(\alpha\beta) = N(\alpha)N(\beta)$.

Consideriamo i numeri complessi della forma $a + bi$, con a e b interi. Questi numeri complessi si chiamano *interi di Gauss*; l'insieme di questi numeri è un anello, come subito si verifica, e si denota con $Z[i]$. Non si tratta di un campo, e anzi i soli elementi invertibili sono $1, -1, i, -i$. Questi elementi sono invertibili:

$$1 = 1 \cdot 1 = (-1)(-1) = i(-i).$$

E sono i soli. Infatti, sia $\alpha = a + bi$ invertibile, e $\alpha\beta = 1$, $\beta = c + di$. Considerando le norme di α e di β, si ha $(a^2 + b^2)(c^2 + d^2) = 1$, da cui $a^2 + b^2 = 1$. Ma trattandosi di una somma di quadrati di interi, ciò implica $a = 0$, $b = \pm 1$ oppure $b = 0, a = \pm 1$, e il risultato.

Il fatto più interessante riguardante gli interi di Gauss è che si tratta di un anello nel quale si può eseguire la divisione euclidea, proprio come nel caso degli interi. Il ruolo che ha il resto nel caso degli interi qui lo ha la norma.

Teorema 1. *Dati due interi di Gauss $\alpha = a + bi$ e $\beta = c + di$, esistono due interi di Gauss κ e ρ tali che $\alpha = \beta\kappa + \rho$ e $N(\rho) < N(\beta)$.*

Dim. Intanto, dati i due numeri complessi α e $\beta \neq 0$, esiste un numero complesso γ tale che $\alpha = \beta\gamma$. Nel caso di α e β interi di Gauss, si può intanto dimostrare che γ è a coefficienti razionali. Infatti, sia $\gamma = \gamma_1 + \gamma_2 i$. Allora:

$$a + bi = (c + di)(\gamma_1 + \gamma_2 i) = (c\gamma_1 - d\gamma_2) + (c\gamma_2 + d\gamma_1)i,$$

da cui il sistema in γ_1 e γ_2:

$$\begin{aligned} c\gamma_1 - d\gamma_2 &= a, \\ c\gamma_2 + d\gamma_1 &= b \end{aligned}$$

che ha soluzioni razionali. Ora, dato un numero razionale $\frac{a}{b}$, esiste un intero n tale che $|n - \frac{a}{b}| \leq \frac{1}{2}$ (vedi Nota seguente). Siano $|n-\gamma_1| \leq \frac{1}{2}$, $|m-\gamma_2| \leq \frac{1}{2}$. Posto $s = \gamma_1 - n$, $t = \gamma_2 - m$ si ha:

$$\alpha = \beta(\gamma_1 + \gamma_2 i) = \beta(s+n) + \beta(t+m)i = \beta(n+mi) + \beta(s+ti)$$

da cui $\beta(s+ti) = \alpha - \beta(n+mi) \in Z[i]$. Posto $\kappa = n + mi$ e $\rho = \beta(s+ti)$, abbiamo i κ e ρ richiesti. Resta da dimostrare che $N(\rho) < N(\beta)$. Si ha:

$$N(\rho) = N(\beta) \cdot N(s+ti) = N(\beta)(s^2+t^2) \leq N(\beta)(\frac{1}{4} + \frac{1}{4}) \leq N(\beta)\frac{1}{2} < N(\beta).$$

Il teorema è così dimostrato. □

Nota. Ricordiamo che nella divisione di a per b, si considerano i multipli di b:

$$\ldots, -kb, \ldots, -2b, -n, 0, b, 2b, \ldots, kb, \ldots$$

e due termini consecutivi di questa successione qb e $(q+1)b$ tali che $qb \leq a < (q+1)b$ (q è il quoziente, e $r = a - bq$ il resto). Sia $r' = b(q+1) - a$; allora $r + r' = b$. I numeri $2r$ e $2r'$ non possono essere entrambi superiori a b; altrimenti $2r + 2r' > 2b$, da cui $r + r' > b$.

Gli interi di Gauss si possono rappresentare nel piano dei numeri complessi. Essi corrispondono ai punti di coordinate intere, e pertanto determinano una quadrettatura di lato 1 di tale piano.

Si ha quindi la seguente interpretazione geometrica del procedimento della divisione.

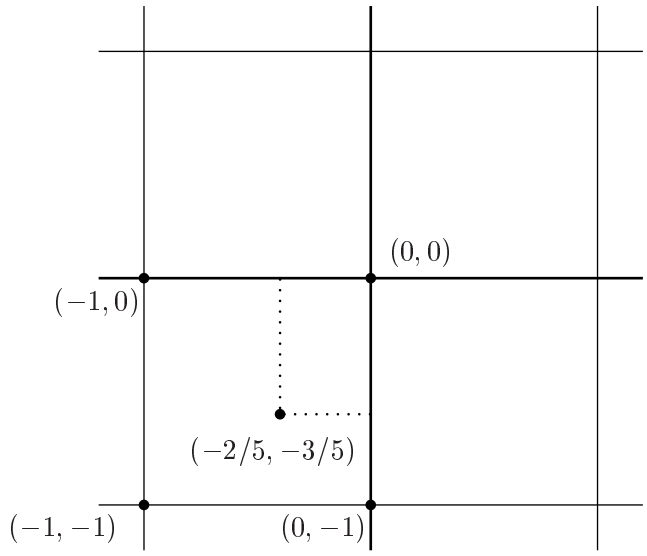
1. Dati due interi di Gauss α e β si prende il quoziente $\gamma = \alpha/\beta$ nel campo complesso (che esiste sempre perché siamo appunto in un campo).

2. Si dimostra che γ è a coefficienti razionali, in generale non interi, e pertanto il punto che lo rappresenta non è in generale uno dei vertici della quadrettatura, a meno che γ non sia un intero di Gauss.

3. Lo scopo è trovare un intero di Gauss q, quindi uno dei vertici della quadrettatura, che sia vicino ad α/β, dove per "vicino" si intende che il resto della divisione sia di norma inferiore a b. Un altro modo di dire la stessa cosa è: "si cerca un intero di Gauss $q = n + mi$ tale che la distanza tra $\gamma = \alpha/\beta$ e q, sia inferiore a 1". Con la scelta dei due interi n ed m che distano da γ_1 e γ_2, rispettivamente, per meno di 1/2, la differenza tra le ascisse e le ordinate di γ e q è $\sqrt{(1/2)^2 + (1/2)^2} < 1$. Tutti e quattro i vertici del quadrato in cui cade α/β possono essere candidati. Il quoziente, quindi, in generale *non è unico* (e di conseguenza nemmeno il resto lo è). È unico se e solo se α/β

cade in uno dei vertici della quadrettatura, cioè se e solo se i suoi coefficienti sono interi, cioè se è un intero di Gauss.

Ad esempio, con $\alpha = 3 - 2i$ e $\beta = 5i$, si ha[1] $\gamma = \alpha/\beta = (-2/5) - (3/5)i$. Questo numero complesso si trova all'interno del quadrato di vertici $(0,0), (-1,0), (-1,-1), (0,-i)$, corrispondenti, rispettivamente, agli interi di Gauss $0, -1, -1-i, -i$.



La distanza di γ da ciascuno dei quattro vertici è minore di 1. La distanza tra due punti si calcola infatti come la radice quadrata della somma dei quadrati delle differenze delle coordinate omonime: ad esempio, la distanza del punto $(-2/5, -3/5)$ da $(-1, -i)$ è

$$\sqrt{(-\frac{2}{5}+1)^2 + (-\frac{3}{5}+1)^2} = \sqrt{(\frac{3}{5})^2 + (\frac{2}{5})^2} = \sqrt{\frac{13}{25}} = \frac{\sqrt{13}}{5} \sim 0.721\ldots < 1.$$

Pertanto abbiamo quattro quozienti:

$$3 - 2i \quad = \quad 5i \cdot (0) + (3 + 2i), N(3+2i) = 3^2 + 2^2 = 13 < N(5i) = 25,$$

[1] Ricordiamo che per trovare il quoziente di due numeri complessi α/β basta moltiplicare α e β per il coniugato di β:

$$\frac{a+bi}{c+di} = \frac{a+bi}{c+di} \cdot \frac{c-di}{c-di} = \frac{ac+bd}{c^2+d^2} + \frac{bc-ad}{c^2+d^2} i.$$

$$
\begin{aligned}
&= 5i(-1) + (3+3i),\ N((3+3i) = 3^2 + 3^2 = 18 < N(5i),\\
&= 5i(-1-i) + (-2+3i),\ N(-2+3i) = (-2)^2 + 3^2 = 13 < N(5i),\\
&= 5i(-i) + (-2-2i),\ N(-2-2i) = (-2)^2 + (-2)^2 = 8 < N(5i).
\end{aligned}
$$

Nel caso dei numeri interi (ma visti come numeri razionali) procedimento è analogo. Vediamo come operare la divisione di due interi seguendo il procedimento usato per gli interi di Gauss:

1. si considera il numero razionale a/b;

2. si cerca un intero q (che sarà il quoziente) tale che la differenza ("la distanza") tra a/b e q sia inferiore a 1;

3. se $a/b - q = t < 1$, si ha $a - bq = bt < b$, e con $bt = r$ si ha $a = bq + r$, $0 \leq r < b$. Ad esempio, con $a = 13$ e $b = 5$, abbiamo, con $q = 2$, $13/5 - 2 = 3/5$, e $13/5 - 2 = 3/5 < 1$.

Con la divisione, negli interi di Gauss abbiamo anche l'algoritmo di Euclide: esso ha sempre termine perché le norme dei resti successivi vanno diminuendo, ed essendo le norme interi non negativi, si giunge certamente a un resto nullo. Inoltre, un intero di Gauss può avere solo un numero finito di divisori: se α divide β, allora $N(\alpha)$ divide $N(\beta)$, per cui β ha solo un numero finito di divisori, essendo questo il caso dell'intero $N(\beta)$. Un dominio nel quale vale la divisione euclidea con resto si chiama *anello euclideo*. $Z[i]$ è quindi un anello euclideo. Formalmente, un anello euclideo è un dominio d'integrità D nel quale per ogni $0 \neq a \in D$ è definito un intero non negativo $v(a)$, detto *valutazione* di a, tale che:

1. Se $a, b \in D$ non entrambi zero, $v(a) \leq v(ab)$;
2. se $a, b \in D$, $b \neq 0$, esistono q, r tali che $a = bq + r$ con $r = 0$ oppure $v(r) < v(b)$.

Riassumiamo gli esempi che conosciamo:

1. Gli interi Z con $v(n) = |n|$;
2. I polinomi sopra un campo, con $v(f) = \partial f$.
3. Gli interi di Gauss, con $v(\alpha) = N(\alpha)$.

Per un anello euclideo si ha questo risultato generale:

Teorema 2. *Un anello euclideo è un anello a ideali principali.*

Dim. La dimostrazione è del tutto analoga a quella per gli interi. Il ruolo di un elemento minimo nell'ideale è assunto, nel caso generale, da un elemento a valutazione minima. □

2 Unità ed elementi associati

In un dominio'integrità D si dice che a *divide* b in D (in simboli, $a|b$), se esiste $c \in D$ tale che $ac = b$, e che b è *associato* ad a in R se contemporaneamente $a|b$ e $b|a$. In particolare, $a|1$ significa che a ha un inverso in R, e quindi che a è *invertibile* in R. Gli elementi associati a 1 sono quindi gli elementi invertibili di R. La relazione $a|b$ è riflessiva e transitiva; la relazione "a è associato a b" è anche simmetrica, e perciò è di equivalenza.

In un dominio di integrità D, a e b sono associati se e solo se $a = bu$ per qualche u invertibile. Infatti, se $a|b$ e $b|a$ esistono c e d tali che $ac = b$ e $bd = a$; ne segue $acd = a$. Se $a \neq 0$, la regola di cancellazione fornisce $cd = 1$, per cui c e d sono invertibili. Se $a = 0$, anche $b = 0$, per cui $a = b \cdot 1$, con 1 che è invertibile. Viceversa, da $a = bu$ con u invertibile si ha $b = au^{-1}$, e quindi $a|b$ e $b|a$. Un elemento invertibile $u \in D$ si dice anche *unità*, e si dice che è un divisore dell'unità 1 (unità fondamentale). Un divisore di un'unità è ancora un'unità (è anch'esso un divisore di 1); una potenza di un'unità è ancora un'unità. Il reciproco di un'unità è ancora un'unità. Un qualunque elemento di D è divisibile per tutti i suoi associati e tutti gli invertibili (che sono gli associati di 1): questi sono i divisori *impropri* di 1 in D. Se $a \neq 0$ non ha divisori propri in D e non è invertibile in D, allora a si dice *irriducibile*.

Se D è un campo, ogni elemento non zero è invertibile, e quindi nessun elemento è irriducibile.

In Z, i soli invertibili sono 1 e –1, e quindi due interi m ed n sono associati se e solo se $m = \pm n$. Un intero p è primo in Z se e solo se i suoi soli divisori sono ± 1 e $\pm p$.

Nell'anello dei polinomi sopra un dominio D (in particolare sopra un campo) il prodotto di due polinomi fg ha grado la somma dei gradi, e coefficiente direttore il prodotto dei coefficienti direttori, e quindi $fg = 1$ solo se f, g sono entrambi costanti, e quindi invertibili in D. Due polinomi sono associati se e solo se $g = cf$, con c costante invertibile in D.

Negli interi di Gauss vi sono quattro unità: $1, i, -1, -i$; si ha $1 = (-1)(-1) = i(-i)$. E sono le sole; infatti, se $1 = \alpha\beta$, deve aversi $1 = N(1) = N(\alpha)N(\beta)$, da cui $N(\alpha) = a^2 + b^2 = 1, a = \pm 1, b = \pm 1$, e si hanno i quattro elementi detti. Un intero di Gauss $a + bi$ ha allora quattro associati: $a + bi, -a - bi, -b + ai, b - ai$

Nell'anello $Z[\sqrt{2}]$ formato dai numeri reali della forma $a + b\sqrt{2}$, con a, b interi, il numero $1 + \sqrt{2}$ è un'unità; infatti $1 = (1 + \sqrt{2})(-1 + \sqrt{2})$. (nel caso di $Z[\sqrt{2}]$, ad esempio, sono unità gli infiniti numeri $(1 \pm \sqrt{2})^n$);

Esempi. Negli interi di Gauss, sia $\beta = 3+i$, e cerchiamo i suoi divisori. Si ha

$N(\beta) = 3^2 + 1^2 = 10$, ed essendoci due decomposizioni di 10, cioè $10 = 1 \cdot 10$ e $10 = 2 \cdot 5$, cerchiamo tra gli $\alpha = a + bi$ tali che $N(\alpha) = 1$ e $N(\alpha) = 2$, ovvero $a^2 + b^2 = 1$ e $a^2 + b^2 = 2$. Queste uguaglianze hanno le soluzioni, la prima, $a = \pm 1, b = 0$ e $a = 0, b = \pm 1$; la seconda $a = \pm 1, b = \pm 1$. I divisori sono allora $\pm 1, \pm i, \pm 1 \pm i$. Si ha,

$$\begin{aligned} 3 + i &= 1 \cdot (3 + i) = -1 \cdot (-3 - i) = i \cdot (1 - 3i) = -i \cdot (-1 + 3i) \\ &= (1 + i)(2 - i) = (-1 - i)(-2 + i) = (1 - i)(1 + 2i) \\ &= (-1 + i)(-1 - 2i). \end{aligned}$$

Otteniamo così sedici divisori di $3+i$. In realtà, quelli essenzialmente distinti sono quattro: $1, 1 + i, 2 - i, 3 + i$; gli altri dodici sono associati di questi.

Come nel caso degli interi naturali, ci si può chiedere quali sono i numeri *primi* nei numeri interi di Gauss: *un intero di Gauss è primo se non si può decomporre in due fattori di norma minore.* Si può quindi avere una decomposizione di un primo di Gauss α ma solo nella forma $\alpha = \beta\gamma$, dove β o γ è un'unità

Esempi. 1. Il numero 5 non è un primo di Gauss: si spezza infatti in $(1 + 2i)(1 - 2i)$.

2. Il numero 3, invece, è primo. Infatti, sia $3 = \alpha\beta$, $\alpha, \beta \in Z[i]$. Allora $N(\alpha)N(\beta) = 9$, per cui o $N(\alpha) = 3$ e $N(\beta) = 3$. Ma 3 non è una somma di quadrati di interi. Si hanno le fattorizzazioni (fittizie) con i quattro elementi invertibili: $3 = 1 \cdot 3 = -1 \cdot (-3) = i \cdot (-3i) = -i \cdot 3i$.

3. Se $\alpha + bi$ è primo, anche il suo coniugato $\overline{\alpha} = a - bi$ lo è. Infatti, se $\overline{\alpha} = \beta\gamma$, prendendo i coniugati si ha $\alpha = \overline{\beta}\overline{\gamma}$, e α non sarebbe più primo.

Teorema 3. *Se $N(\alpha)$ è un numero primo ordinario, α è un numero primo di Gauss.*

Dim. Se $\alpha = \beta\gamma$, dove β e γ non sono unità, si avrebbe $N(\alpha) = N(\beta)N(\gamma)$, con $N(\beta), N(\gamma) > 1$ ed $N(\alpha)$ non sarebbe primo. □

Il viceversa è falso: 3 è primo come intero di Gauss, ma è di norma 9, che non è primo.

Quali sono i numeri primi p che sono norme di interi di Gauss, cioè che sono somme di due quadrati? Se $p = 2$, $2 = (1 + i)(1 - i)$, e quindi 2 è norma di $1 + i$ e dei suoi associati. Se p è dispari, e $p \equiv 3 \bmod 4$, allora p non è mai somma di quadrati: se $p = a^2 + b^2$, a e b devono essere uno pari e uno dispari: $(2h)^2 + (2k + 1)^2 = 4h^2 + 4k^2 + 4k + 1 \equiv 1 \bmod 4$. Dunque, come visto sopra per 3, i primi della forma $3 + 4n$ (3,7,11,15,...) sono primi anche come interi di Gauss. Si può dimostrare (teorema di Fermat) che

invece i primi della forma $1+4n$ sono somme di due quadrati (ad esempio, $13 = 1 + 4 \cdot 3 = 2^2 + 3^2$).

In $Z[i]$ consideriamo l'elemento $i-2$, l'ideale $(i-2)$ da esso generato, e vediamo di determinare il quoziente $Z[i]/(i-2)$. Come osservato nella precedente dispensa, considerare questo quoziente significa considerare in $Z[i]$ la relazione $i-2=0$, cioè $i=2$. Elevando al quadrato si ha $i^2 = -1 = 4$, cioè $5 = 0$. In altri termini, la classe in cui sta 5 è lo zero del quoziente $Z[i]/(i-2)$ (e infatti, 5 è un multiplo di $i-2$: $5 = (i-2)(i+2)$. Nel quoziente, allora, abbiamo $i = 3$ e $5 = 0$ per cui, nel quoziente, un generico elemento $a+bi$ di $Z[i]$ diventa $a+3i$, e poiché $5=0$, si tratta di uno tra 0,1,2,3 e 4. È facile allora supporre che il quoziente $Z[i]/(i-2)$ sia isomorfo all'anello delle classi resto mod 5. Verifichiamo, che la corrispondenza $Z[i] \to Z_5$ è surgettiva: ad esempio, la classe 4 mod 5 proviene dalla classe di $3-7i \bmod (i-2)$; posto $i=2$ si ha $3-7\cdot 2 = -11$, cioè è la classe 4 mod 5)), e così per le altre classi mod 5.

3 Fattorizzazione unica

Ogni intero si scrive in modo unico come prodotto di primi. Ad esempio, $90 = 2\cdot 3\cdot 3\cdot 5$, e questa scrittura è unica a meno dell'ordine in cui compaiono i primi. Lo stesso accade nell'anello dei polinomi sopra un campo.

In un dominio D a ideali principali, dati $a, b \in D$, un elemento d si dice massimo comun divisore di a e b, $MCD(a,b)$, se $d|a$ e $d|b$,e per ogni $c \in D$ tale che $c|a$ e $c|b$, si ha $c|d$.

Teorema 4. *In un dominio D a ideali principali, ogni coppia di elementi a,b non nulli ammette un MCD d che si scrive come combinazione lineare di a e b:*

$$d = sa + tb, \tag{1}$$

con opportuni coefficienti $s, t \in R$.

Dim. L'insieme di tutte le combinazioni lineari $xa+yb$ di a e b è un ideale I, come subito si vede, ed è quindi principale: $I=(d)$, per un certo d. Come tutti gli elementi di I, questo d ha la forma $sa+tb$, per certi $s,t \in R$. Tutti gli elementi di I sono allora multipli di d, e dunque anche a e b (che sono anch'essi della forma $xa+yb$ con $x=1$ e $y=0$, e rispettivamente $x=0$ e $y=1$) sono multipli di d. Se poi c è un divisore comune di a e b, $a=a'c$, $b=b'c$, allora $d = sa+tb = (sa'+tb')c$ è multiplo di c. Le proprietà richieste per il MCD sono allora soddisfatte da d. □

Corollario. *Se r è irriducibile in un dominio a ideali principali D, $a, b \in D$, allora*:

$$r|ab \Rightarrow r|a \text{ oppure } r|b. \tag{2}$$

Dim. I fattori di r sono solo invertibili o associati, e dunque $MCD(r, a) = r$ o u, invertibile. Nel primo caso, $r|a$; nel secondo scriviamo, utilizzando la (1) e moltiplicando u per il suo inverso, $b = b \cdot 1 = sab + tbr$. Per ipotesi, r divide ab, e quindi entrambi i termini a secondo membro, e pertanto divide b. □

In particolare, se $MCM(a, c) = 1$ e $c|ab$, allora $c|b$.

Poiché la proprietà principale dei numeri interi primi è la (2), diremo che un elemento p di un dominio d'integrità D è *primo* se:

i) è diverso da zero e non è invertibile;

ii) se p divide un prodotto di elementi di D, allora divide uno dei fattori.

Sono queste le proprietà da cui deriva l'unicità della fattorizzazione.

Ricordiamo come si dimostra il teorema fondamentale dell'aritmetica.

Teorema 5. *Ogni intero $a > 1$ si può scrivere come un prodotto*

$$a = \pm p_1 p_2 \cdots p_k, \tag{3}$$

dove $c = \pm 1$, i p_i sono numeri primi positivi, e $k \geq 0$. Questa espressione è unica a meno di dell'ordine dei p_i.

Dim. Dimostriamo che una tale fattorizzazione esiste. Per induzione su n. Se n è primo, il prodotto (3) ha un solo fattore; altrimenti, a ha un divisore proprio $b \neq a$. Allora $a = bb'$, e anche $b' \neq a$. Sia b che b' sono minori di a: per induzione ammettono ciascuno una fattorizzazione in numeri primi. Scrivendo una accanto all'altra le due fattorizzazioni se ne ottiene una per a.

Riguardo all'unicità, supponiamo che si abbia

$$a = \pm p_1 p_2 \cdots p_h = \pm q_1 q_2 \cdots q_k.$$

I segni sono gli stessi nei due membri. Poiché p_1 è primo, e divide il secondo membro, divide uno dei q_i, e sia q_1. Poiché q_1 è primo, $p_1 = q_1$. Cancellando p_1 e procedendo per induzione si ha la tesi. □

Se si cerca un teorema analogo per un dominio d'integrità qualunque, occorre dividere l'enunciato in due parti: *i*) un dato elemento a deve essere

prodotto di elementi irriducibili; *ii*) il prodotto deve essere essenzialmente unico.

Riguardo alla prima parte, occorre supporre che a non sia né zero né un'unità, altrimenti non c'è modo di scriverlo come prodotto di elementi irriducibili. Si procede poi come segue: se a è irriducibile, non c'è altro da dimostrare. Altrimenti, a ammette un fattore proprio, e quindi si decompone come un prodotto $a = a_1 b_1$, dove né a_1 né b_1 sono unità. Continuiamo a fattorizzare a_1 e b_1, se possibile, sperando che il procedimento abbia termine, cioè che dopo un numero finito di passi tutti i fattori sono irriducibili. Il fatto che il procedimento termini ha una precisa espressione in termini di ideali:

Teorema 6. *Sia D un dominio di integrità. Le seguenti condizioni sono equivalenti:*

i) *per ogni $0 \neq a$ che non sia un'unità, il procedimento di fattorizzazione di a termina dopo un numero finito di passi, e si ottiene una fattorizzazione $a = b_1 b_2 \cdots b_k$ di a in elementi irriducibili di D;*

ii) *D non contiene catene ascendenti infinite di ideali principali:*

$$(a_1) \subset (a_2) \subset (a_3) \subset \cdots. \tag{4}$$

In altre parole, ogni catena ascendente di ideali principali è stazionaria, esiste cioè un indice k tale che:

$$(a_1) \subset (a_2) \subset (a_3) \subset \cdots (a_k) = (a_{k+1}) = \cdots$$

Dim. Supponiamo che D contenga una catena come la (4). Nessuno degli ideali (a_n) coincide con $D = (1)$, in quanto $(a_n) \subset (a_{n+1}) \subset (1)$. Poiché $(a_{n-1}) \subset (a_n)$, a_n è un divisore proprio di a_{n-1}; sia $a_{n-1} = a_n b_n$, dove a_n e b_n non sono unità. Si ha così una successione infinita di fattorizzazioni di a_1:

$$a_1 = a_2 b_2 = a_3 b_3 b_2 = a_4 b_4 b_3 b_2 = \ldots.$$

Viceversa, una tale successione di fattorizzazioni fornisce una catena ascendente di ideali come la (4). □

Se in un anello la fattorizzazione è spesso possibile, non è però sempre unica. Ad esempio, nell'anello $Z[\sqrt{-5}]$ dei numeri complessi della forma $a + b\sqrt{-5}$ (ovvero $a + b\sqrt{5}i$), con a e b interi, le unità sono soltanto 1 e -1, e il numero 6 ammette due fattorizzazioni:

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5});$$

tutti e quattro i termini $2, 3, 1+\sqrt{-5}, 1-\sqrt{-5}$ sono irriducibili. Poiché le unità sono 1 e –1, gli associati di 2 sono 2 stesso e –2, per cui 2 non è un associato né di $1+\sqrt{-5}$ né di $1-\sqrt{-5}$.

Abbiamo definito *primo* un elemento di D se non è né zero né un'unità, e se dividendo un prodotto divide uno dei fattori.

Teorema 7. *Se in dominio di integrità esiste la fattorizzazione in irriducibili, essa è unica se e solo se ogni elemento irriducibile è primo.*

Dim. La dimostrazione è la stessa vista per il teorema fondamentale dell'aritmetica. □

È importante distinguere tra irriducibili e primi: vi sono anelli che contengono elementi irriducibili che non sono primi. Ad esempio, in $Z[\sqrt{-5}]$, l'elemento 2 non ha divisori propri, e quindi è irriducibile, ma non è primo perché pur dividendo $6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$ non divide alcuno dei due fattori. Ma si ha:

Teorema 8. *i) In un dominio di integrità, un elemento primo è irriducibile;*
ii) in un dominio a ideali principali, un elemento irriducibile è primo.

Dim. i) Sia p primo, e sia $p = ab$. Allora $p|ab$, ed essendo primo, $p|a$ o $p|b$. Sia $p|a$; allora $a = pt$, da cui $a = (ab)t = a(bt)$. Semplificando a (qui si usa il fatto che siamo in un dominio d'integrità), abbiamo $bt = 1$, e quindi $b|1$, e perciò b è invertibile. Pertanto p non ha divisori propri, e quindi è irriducibile.
ii) Corollario del Teorema 4. □

Teorema 9. *In un dominio D a ideali principali, ogni catena ascendente di ideali:*

$$I_1 \subset I_2 \subset \cdots \subset I_k \subset \cdots$$

è stazionaria, esiste cioè un indice m tale che $I_m = I_{m+1} = \cdots$.

Dim. Dimostriamo che l'unione $I = \bigcup_k I_k$, $k = 1, 2, \ldots$, è un ideale, cioè che è chiuso rispetto alla somma e al prodotto per un elemento dell'anello. Se $a, b \in I$, allora $a \in I_h$ e $b \in I_k$, per certi h e k, e dunque a e b appartengono al più grande tra i due, il quale essendo un ideale, contiene anche $a + b$. Allora $a + b \in I$, e I è un sottogruppo del gruppo additivo dell'anello. Se $a \in I$ ed $r \in D$, allora $a \in I_h$ per un certo h, ed essendo I_h un ideale anche $ar \in I_h$, e pertanto $ar \in I$. Come tutti gli ideali di D, I è principale: $I = (a)$, per un certo $a \in D$. Ma essendo $I = \bigcup_k I_k$, a appartiene a uno degli ideali dell'unione, e sia I_m. Ne segue $I_m = I$, e dunque $I_m = I_{m+1} = \cdots$. □

Se in un anello (qualunque, non necessariamente un dominio) ogni catena ascendente di ideali è stazionaria, si dice che l'anello soddisfa la *condizione della catena ascendente* (CCA).

Dai teoremi 6, 7, 8 e 9 abbiamo ora:

Teorema 10. *Un dominio a ideali principali è un dominio a fattorizzazione unica.*

Nota. Nel caso degli interi (Teorema 5), l'unicità della fattorizzazione é stata dimostrata usando l'induzione. Nel caso di un dominio a ideali principali qualunque l'induzione viene sostituita dalla CCA.

Il viceversa del Teorema 9 è falso. L'anello dei polinomi a coefficienti interi $Z[x]$ è un dominio a fattorizzazione unica, ma esistono ideali che non sono principali (ad esempio, l'ideale $(2, x)$ dei polinomi a termine noto pari).

La nozione duale di MCD è quella di minimo comune multiplo. Un elemento $m \in D$ è un *minimo comune multiplo* di $a, b \in D$, $mcm(a, b)$, se è un multiplo comune di a e b che divide tutti i multipli comuni di a e b

$$a|m,\ b|m \text{ e } a|e,\ b|e \Rightarrow m|e$$

(nel caso del MCD d si ha "d è multiplo di tutti i divisori comuni"; qui si ha "m divide tutti i multipli comuni). In un dominio a ideali principali, un tale elemento m esiste sempre. Infatti, i multipli comuni di a e b formano un ideale, che quindi è principale e generato da un elemento m che ha le proprietà del *mcm*.

4 Polinomi sul campo razionale

Definizione. Un polinomio a coefficienti interi si dice *primitivo* se il MCD dei coefficienti è 1.

Teorema 11. *Il prodotto di due polinomi primitivi f e g è primitivo.*

Dim. Se il prodotto fg non è primitivo, sia p un primo che divide tutti i coefficienti. Consideriamo l'omomorfismo $Z[x] \to Z_p[x]$, che associa a un polinomio f a coefficienti interi lo stesso polinomio ma con i coefficienti modulo p, $\bar{f}$. Per ipotesi, $\overline{fg} = \overline{f} \cdot \overline{g} = 0$, e quindi o $\bar{f} = 0$ o $\bar{g} = 0$, ma ciò significa che o f o g non è primitivo. □

Teorema 12 (Lemma di Gauss). *Se un polinomio primitivo f si fattorizza sui razionali, allora si fattorizza anche sugli interi.*

Dim. Se $f = uv$, u, v polinomi a coefficienti razionali, allora riducendo i coefficienti allo stesso denominatore e mettendo in evidenza i fattori comuni si ha $f = (a/b)\lambda\mu$, a, b interi, λ, μ polinomi a coefficienti interi e primitivi; per il lemma, $\lambda\mu$ è primitivo. Allora $bf = a\lambda\mu$. Il MCD dei coefficienti di bf è b in quanto f è primitivo; quello di $a\lambda\mu$ è a in quanto $\lambda\mu$ è primitivo. Allora $a = b$ e $f = \lambda\mu$, con λ, μ polinomi a coefficienti interi. □

Teorema 13 (Criterio di Eisenstein). *Sia $a_0 + a_1x + a_2 + \cdots + a_nx^n$ a coefficienti interi, e supponiamo che esista un primo p tale che p non divide a_n, p divide tutti gli altri coefficienti, e p^2 non divide a_0. Allora il polinomio è irriducibile sui razionali.*

(Ad esempio, $2x^5 - 6x^3 + 9x^2 - 15$ è irriducibile su Q: soddisfa il criterio con $p = 3$).

Dim. Se f si fattorizza su Q, si fattorizza su Z (Lemma di Gauss). Sia $f = uv$ su Z, e prendiamo i polinomi modulo p. f diventa ax^n, (a è la classe resto di a_n mod p) e poiché il polinomio x^n si fattorizza in monomi, e la fattorizzazione è unica, gli unici fattori di x^n sono del tipo x^h: abbiamo allora $ax^n = bx^k \cdot cx^{n-k}$. Ma ciò significa che mod p, i termini noti di u e v sono zero, cioè che questi termini noti sono divisibili per p, e allora il termine noto di f è divisibile per p^2, contro l'ipotesi. □

Ricordiamo che un criterio è una condizione *sufficiente*, non necessaria. In altre parole, un polinomio può essere irriducibile anche se il criterio non si applica. Ad esempio, $x^2 + 2x + 4$ è irriducibile, ma non vi è alcun primo che soddisfi l'enunciato del teorema.

In alcuni casi si vede subito se il criterio si applica. Ad esempio, nel caso del polinomio $x^n - p$, per ogni numero primo p. In altri casi, a prima vista il criterio può non essere applicabile; ma con un cambiamento di variabile si può trasformare il polinomio in modo da renderlo applicabile. L'idea è la seguente. È chiaro che se un polinomio $f(x)$ si spezza, $f(x) = g(x)h(x)$, lo stesso accade per $f(x + m)$, che si spezza in $f(x + m) = g(x + m)h(x + m)$. Con la sostituzione di $x + m$ a x il criterio può diventare applicabile. Ad esempio, sia $f(x) = x^2 + x + 2$; il criterio non è applicabile. Ma consideriamo $f(x + 3) = x^2 + 7x + 14$; questo soddisfa il criterio con $p = 7$, e pertanto è irriducibile, e quindi anche $f(x)$ lo è.

Un caso famoso di applicazione di questa tecnica di passaggio da x a $x + m$ per un certo intero m è quello del polinomio ciclotomico relativo al primo p. (Parleremo più in generale di polinomi ciclotomici nel prossimo paragrafo).

Teorema 14. *Il polinomio ciclotomico:*

$$f(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdot + x + 1$$

è irriducibile.

Dim. Eisenstein non è applicabile. Ma consideriamo $f(x+1)$. Si ha:

$$f(x+1) = \frac{(x+1)^p - 1}{(x+1) - 1} = \frac{(x+1)^p - 1}{x}.$$

Ora,

$$(x+1)^p = \sum_{k=0}^{p} \binom{p}{k} x^k = 1 + \binom{p}{1} x + \binom{p}{2} x^2 + \cdots + \binom{p}{p-1} x^{p-1} + x^p$$

per cui

$$f(x+1) = p + \binom{p}{2} x + \cdots + \binom{p}{p-1} x^{p-2} + x^{p-1}.$$

Ma per $\binom{p}{k} = p!/k!(p-k)!$, e per $0 < k < p$, questo numero è divisibile per p. Si può allora applicare il criterio di Eisenstein a $f(x+1)$, e concludere che il polinomio ciclotomico relativo a p è irriducibile. □

Esempio. Per $p = 3$, il polinomio ciclotomico è $x^2 + x + 1$, al quale il criterio non si applica. Con il cambiamento di variabile $x \to x + 1$ abbiamo:

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

e ora il criterio si applica.

5 Il polinomio ciclotomico

Il polinomio $x^n - 1$ a coefficienti razionali è il polinomio le cui radici sono le radici $n-$esime dell'unità. Queste si dispongono sul cerchio unitario del piano complesso dividendolo in parti uguali (unendo in successione i punti dove si trovano le radici si ottiene un poligono regolare di n lati). Il polinomio ha le n radici $\alpha_k = e^{2k\pi i/n} = (e^{2\pi i/n})^k, k = 0, 1, \ldots, n-1$, che come si vede si ottengono tutte come potenze di una di esse, $e^{2\pi i/n}$: si tratta di un gruppo ciclico, generato da $e^{2\pi i/n}$. Una radice $(e^{2\pi i/n})^k$ genera tutte le altre se e solo se $(k, n) = 1$; queste radici si dicono *primitive*, e sono in numero di $\varphi(n)$, la funzione di Eulero di n.

Il polinomio *ciclotomico* $\Phi_n(x)$ è il polinomio le cui radici sono le radici primitive $n-$esime dell'unità[2]:

$$\Phi_n(x) = \prod_{(k,n)=1} (x - \alpha_k). \tag{5}$$

e perciò ha grado $\varphi(n)$.

Se d è un divisore di n, e α è una radice primitiva $n-$esima, allora $\alpha^{n/d}$ è una radice primitiva $d-$esima dell'unità. Definiamo allora, analogamente, $\Phi_d(x)$ come il prodotto di tutti i fattori lineari $x - \beta$, dove β varia tra le radici primitive $d-$esime dell'unità. Ne segue

$$x^n - 1 = \prod_{d|n} \Phi_d(x). \tag{6}$$

Esempi. $x^4 - 1$ ha le radici $1, -1, i, -i$, e i e $-i$ sono le primitive. Dunque:

$$\Phi_4(x) = (x - i)(x + i) = x^2 + 1.$$

La sola radice primitiva seconda dell'unità è –1; e dunque:

$$\Phi_2(x) = x + 1,$$

e l'unica radice prima dell'unità è 1, e quindi:

$$\Phi_1(x) = x - 1.$$

Nota. Prendendo i gradi dei due membri della (6) abbiamo:

$$n = \sum_{d|n} \varphi(d),$$

e questa permette di calcolare la funzione di Eulero $\varphi(n)$ in modo ricorsivo, cioè a partire dalla conoscenza dei valori precedenti. Ad esempio, volendo conoscere $\varphi(15)$, conoscendo $\varphi(k)$ per $k < 15$ abbiamo:

$$15 = \varphi(1)\varphi(3)\varphi(5)\varphi(15) = 1 + 2 + 4 + \varphi(15),$$

da cui $\varphi(15) = 15 - 7 = 8$.

[2]Si dà a questo il nome di polinomio ciclotomico (che significa "polinomio della divisione del cerchio") anche se sono le radici $x^n - 1$ che dividono il cerchio in n parti uguali.

Teorema 15. *Il polinomio ciclotomico $\Phi_n(x)$ su Q è a coefficienti interi.*

Dim. Per induzione su n. Se $n = 1$, $\Phi_1(x) = x - 1$, che è a coefficienti interi. Supponiamo il teorema vero per $\Phi_m(x)$, $m < n$. Per la (1) abbiamo:

$$x^n - 1 = (\prod_{d|n, d<n} \Phi_d(x)) \cdot \Phi_n(x).$$

Per induzione, i $\Phi_d(x)$ sono a coefficienti interi, e dunque il loro prodotto lo è, e poiché i coefficienti direttori dei $\Phi_d(x)$ sono uguali a 1, anche il prodotto $\prod_{d|n,d<n} \Phi_d(x)$ ha coefficiente direttore 1. Il quoziente di $x^n - 1$ per questo prodotto è allora a coefficienti interi, e questo quoziente è proprio $\Phi_n(x)$. □

6 Alcuni risultati sui polinomi

Teorema fondamentale dell'Algebra. *Il campo complesso* **C** *è algebricamente chiuso, cioè: un polinomio non costante a coefficienti complessi ha una radice in* **C**.

Teorema 16. *Un polinomio $f(x)$ su un campo F che ha una radice a in F è divisibile per $x - a$.*

Dim. Dividendo $f(x)$ per $x - a$ abbiamo $f(x) = (x - a)q(x) + r(x)$, con $0 \leq \delta r < 1$, cioè r costante, oppure $r = 0$, cioè r è il polinomio identicamente nullo. Se $r = 0$, non c'è più niente da dimostrare. Altrimenti, calcolando in a abbiamo $0 = f(a) = (a-a)r(a)$, e quindi $r(a) = 0$, ed essendo $r(x)$ costante, se una volta assume il valore 0 lo assume sempre. Ne segue $r(x) = 0$, e $f(x) = (x - a)q(x)$. □

Si dice che $f(x)$ ha la radice a di *molteplicità* (almeno) m se $(x - a)^m$ divide $f(x)$.

Teorema 17. *Un polinomio di grado n a coefficienti in un campo o è nullo, oppure se è di grado n ha al più n radici nel campo o in un suo ampliamento.*

Dim. Induzione su n. Se $n = 1$, $f(x) = ax+b$ ha la sola radice $x = -b/a$. Se $\delta f > 1$, e $f(x)$ non ha radici, non c'è niente da dimostrare. Sia a una radice; allora $f(x)$ è multiplo di $x - a$ (Teorema 16): $f(x) = (x - a)q(x)$. Se $b \neq a$ è un'altra radice di $f(x)$, allora $0 = f(b) = (b - a)q(b)$, ed essendo $b \neq a$, è $q(b) = 0$, ovvero b è radice di $q(x)$. l polinomio $q(x)$, che ha grado $n - 1$, per induzione ha al più $n - 1$ radici, e queste sono anche radici di $f(x)$. Aggiungendo a, $f(x)$ ha al più n radici. □

Corollario 1. *Un polinomio $f(x)$ di grado n a coefficienti complessi ha esattamente n radici in* $\mathbf{C}$ *(contando le molteplicità).*

Dim. Per il teorema fondamentale dell'algebra, il polinomio f ha almeno una radice $a \in \mathbf{C}$. Per il Teorema 17, $f(x)$ è divisibile per $x - a$: $f(x) = (x - a)q(x)$, con $\delta q = n - 1$. Per induzione, q ha esattamente $n - 1$ radici, che sono anche radici di f. Aggiungendo a, f ha esattamente n radici. □

Corollario 2. *Se due polinomi f e g di grado al più n assumono gli stessi valori per $n + 1$ valori distinti della variabile, allora essi coincidono.*

Dim. Il polinomio $f - g$ ammette $n+1$ radici. Se non è il polinomio nullo, ha un grado, e questo grado è al più n. Ma allora, per il Teorema 17, non può avere più di n radici. Ne segue $f - g = 0$ e $f = g$. □

In particolare, un polinomio $f(x)$ di grado al più n è determinato una volta assegnati i suoi valori $u_0, u_1, \ldots, u_n$ su $n+1$ punti distinti $x_1, x_2, \ldots, x_n$: $f(x_i) = u_i$, $i = 0, 1, 2, \ldots, n$ (se è anche $g(x_i) = u_i$, allora $f(x) - g(x)$ ha grado al più n e sia annulla sugli $n + 1$ punti x_i, e pertanto è il polinomio nullo, per cui $f(x) = g(x)$). Ciò dimostra l'unicità. Si dimostra che un tale polinomio esiste con metodi di interpolazione (*interpolazione di Lagrange*).

Teorema 18. *Siano $f, g \in Q[x]$, con f irriducibile. Se se f e g hanno una radice (complessa) in comune, allora f divide g.*

Dim. Se f non divide g, il MCD tra f e g è 1. Ma allora $f(x)h(x) + g(x)k(x) = 1$, e calcolando nella radice si ottiene l'assurdo $0 = 1$. □

Teorema 19. *I soli polinomi irriducibili a cefficienti reali hanno grado* 1 *o* 2*.*

Dim. Se il grado è 1, è ovvio. Altrimenti, sia $f = ax^2+bx+c$ con $\Delta = b^2 - 4ac$. Se $\Delta \geq 0$, abbiamo due radici reali $\alpha_{1,2} = (-b \pm \sqrt{b^2 - 4ac})/2a$, e il polinomio f si fattorizza in $\alpha_{1,2} = (-b \pm \sqrt{b^2 - 4ac})/2a$, e $f = a(x-\alpha_1)(x-\alpha_2)$. Se $\Delta < 0$, allora α_1 e α_2 sono complesse, e si ha la detta fattorizzazione sui complessi, e poiché la fattorizzazione sui complessi è unica, non può esistere un'altra fattorizzazione sui reali (i numeri reali sono particolari numeri complessi). Ne segue che esistono polinomi di grado 2 irriducibili sui reali, quelli appunto con $\Delta < 0$.

Viceversa, sia f irriducibile, e dimostriamo che ha grado al più 2. Sia $\alpha = a + bi$ una radice complessa (non può essere reale per l'ipotesi di irriducibilità), e sia $g(x) = (x-\alpha)(x-\overline{\alpha}) = x^2 - 2a + a^2 + b^2$. Dividiamo f per g, e calcoliamo in α: $0 = f(\alpha) = g(\alpha)q(\alpha) + r(\alpha) = r(\alpha)$, con $0 \leq \partial r \leq 1$

oppure r nullo. Se $\partial r = 1$, $r(x) = cx + d$, c, d reali, si ha $r(\alpha) = 0$, $c\alpha + d = 0$ e $\alpha = -c/d$. Ma $-c/d$ è reale, contro l'ipotesi che α sia complesso non reale. Ne segue che r è il polinomio nullo, e dunque $f = gq$, oppure r è una costante, che annullandosi una volta, non può che essere zero, e quindi ancora $f = gq$. Ma essendo f irriducibile, q è una costante, e quindi non ha radici. Ne segue $\partial f = \partial g = 2$. □