Capitolo II. FATTORIZZAZIONI IN IRRIDUCIBILI

Premessa lessicale

Anche se il suono è simile, la parola inglese "factoring" non significa calcolare la fattorizzazione (vedi sotto), bensì "passare al quoziente", così come il "factor ring" è l'anello quoziente.
Qui la nostra attenzione è invece puntata sul descrivere un elemento r di un anello R come prodotto di altri o, se si preferisce, sul trovare possibili **divisori** dell'elemento r di R, cioè elementi d tali che per qualche s di R risulti $r=s\ d$. È chiaro che gli elementi invertibili u dividono ogni altro elemento r di R: basta scrivere $r=u\ (u^{-1}\ r)$; è altrettanto chiaro che siamo interessati a trovare divisori più significativi di questi.
All'interno del discorso sulla ricerca di divisori si inseriscono tipici problemi di divisibilità, come quello della ricerca del massimo comun divisore di 2 o più elementi dell'anello (ed eventualmente del loro minimo comune multiplo). Conviene qui richiamarne la definizione.
Siano ***r***, ***s*** *elementi non nulli di* R. *Si dice che* ***d*** *è* ***massimo comun divisore*** *di* ***r*** *e* ***s*** **–** MCD(r,s) **–** *se* ***d*** *divide entrambi gli elementi e ogni altro elemento* ***c*** *di* R *che divida tanto* ***r*** *che* ***s*** *divide anche* ***d***.
Dualmente *si dice che* ***m*** *è* ***minimo comune multiplo*** *di* ***r*** *e* ***s*** **–** mcm(r,s) **–** *se tanto* ***r*** *che* ***s*** *dividono* ***m*** *e, se* ***r*** *ed* ***s*** *dividono un altro elemento* ***c*** *di* R *allora* ***m*** *divide* ***c***. Queste definizioni si estendono per ricorrenza al caso di un numero finito $n > 2$ di elementi.
Anche se non è facile esibire controesempi, non in tutti gli anelli succede che presi comunque 2 elementi non nulli ne esista il MCD: saremo quindi interessati a determinare condizioni che ne garantiscano l'esistenza.
Conviene infine notare che, anche se siamo abituati a dire "il massimo comun divisore" o "il minimo comune multiplo", massimo comun divisore e minimo comune multiplo – quando esistono – sono individuati a meno del prodotto per elementi invertibili e quindi se in R esistono elementi invertibili diversi dall'unità (in particolare se 1+1 non è lo zero di R) ce ne sono più d'uno: come osservato a proposito della nozione di divisore, questo è un inconveniente costante in tutta la teoria della divisibilità, cui in certa misura si cerca di mettere riparo passando dalla considerazione degli elementi a quella degli ideali da essi generati. Comunque questo è un motivo per riservare nel seguito agli elementi invertibili un trattamento particolare.

1. Elementi irriducibili e primi

Sia R un **dominio di integrità**: ogni suo elemento invertibile sarà detto brevemente **unit**. Se si vuole che i discorsi di divisibilità siano significativi bisogna che il dominio R contenga qualche elemento non nullo che non sia un unit (cioè che R non sia un campo): questo implica in particolare che il *dominio* sia *infinito*, visto che i domini finiti sono campi (vedi Capitolo I, osservazione 1.5 j))

DEFINIZIONE 1.1 *Se* $\boldsymbol{r}\in$ R\{0} *non è un unit*, ***r*** *è detto*

- ***primo*** *se ogniqualvolta divide un prodotto* ***a b*** *di elementi di* R *divide almeno uno dei due elementi*;
- ***riducibile*** *se si può scrivere come prodotto di due elementi di* R *entrambi non unit*;
- ***irriducibile*** *se quando è scritto come prodotto di due elementi di* R, *uno dei due è un unit*.

OSSERVAZIONE 1.2 *Ogni elemento primo* ***p*** *è irriducibile*.

Infatti, sia $p=a\ b$; se p divide a, cioè se $a = p\ c$, si vede che $p = p\ c\ b$ da cui, semplificando (cosa lecita visto che R è un dominio), $1 = c\ b$: cioè b è un unit. Se invece p non divide a, visto che divide $a\ b$ ed è primo, deve dividere b, cioè $b = c\ p$: se ne deduce $p = a\ c\ p$, cioè $1 = a\ c$: dunque a è un unit.

Il viceversa non in tutti i domini è vero: si veda l'esempio di $\mathbf{Z}[\sqrt{(-5)}]$ che verrà discusso nel §5.

Ribadiamo che le questioni di divisibilità sono significative per elementi non unit: si cerca però di dare definizioni che possano adattarsi, sia pur banalizzate, al caso di unit. In particolare *una scrittura del tipo*

$$r=u\ r_1\ r_2\ \ldots.\ r_n$$

con $\boldsymbol{u}$ *unit di* R *ed* $\boldsymbol{r}_1, \boldsymbol{r}_2,\ldots,\boldsymbol{r}_n$ *irriducibili* (eventualmente con u=1 o con n=0) *è detta* ***fattorizzazione*** *di* $\boldsymbol{r}$ (in irriducibili).
Se r è un unit la fattorizzazione è data da r stesso $\Rightarrow$ in un campo tutti gli elementi non nulli sono fattorizzabili in maniera unica.
Non sempre, anche in un dominio R in cui tutti gli elementi sono dotati di fattorizzazione, tale fattorizzazione è "unica": si veda ancora l'esempio di $\mathbf{Z}[\sqrt{(-5)}]$.

DEFINIZIONE 1.3 *Un dominio di integrità* R *è detto* ***dominio a fattorizzazione unica*** **(UFD)** *se ogni elemento non nullo e non unit di* R *è dotato di fattorizzazione in irriducibili unica a meno di unit e dell'ordine dei fattori.*

Ad es. in $\mathbf{Z}$ (che, come si vedrà nel paragrafo 3, è un dominio a fattorizzazione unica) $2\ 5$, $5\ 2$, $(-2)\ (-5)$, $(-1)\ (-2)\ 5$ sono pensate tutte come un'unica fattorizzazione di 10 in irriducibili.

Due elementi ***irriducibili*** *che possano essere ottenuti uno dall'altro moltiplicando per un unit* (come 2 e (−2) nel precedente esempio) *saranno detti* ***associati***: è chiaro che "essere associati" è una relazione di equivalenza nell'insieme degli elementi irriducibili di R. Spesso per ogni classe di equivalenza si sceglie un rappresentante "privilegiato" (nel caso di $\mathbf{Z}$ gli irriducibili positivi) e si rappresenta ogni elemento fattorizzabile in irriducibili come prodotto di un sottoinsieme opportuno di questi rappresentanti privilegiati, per un opportuno unit (ad es. $-10=(-1)\ 2\ 5$).

OSSERVAZIONE 1.4 *Sia* $\boldsymbol{r}$ *un elemento non nullo di* R *che ammette una fattorizzazione in irriducibili:* $r = u\ r_1\ r_2\ \ldots.\ r_n$ (con u unit di R). *Se* $\boldsymbol{p}$ *è un elemento primo di* R *che divide* $\boldsymbol{r}$, $\boldsymbol{p}$ *è associato ad (almeno) un* $\boldsymbol{r}_i$.
Infatti p essendo primo divide almeno uno dei fattori irriducibili r_i, in quanto se non divide r_1 divide $(u\ r_1\ r_2\ \ldots.\ r_n)$ e, iterando, se p non divide nessuno degli irriducibili precedenti, deve dividere $(u\ r_n)$ e quindi r_n. D'altra parte p non è un unit e quindi se divide l'elemento irriducibile r_i, deve essere ad esso associato.

Nel successivo paragrafo 3 vedremo esempi significativi di UFD di cui il dominio degli interi è caso particolare (i domini a ideali principali) e nel paragrafo 4 vedremo come costruirne altri a partire da questi.

2. Caratterizzazione degli UFD; mcm e MCD

Abbiamo già osservato che ogni elemento primo è irriducibile. Mostriamo che l'affermazione inversa caratterizza gli UFD.

TEOREMA 2.1 *Sia* R *un dominio di integrità tale che ogni suo elemento non nullo e non unit abbia almeno una fattorizzazione. Sono equivalenti le affermazioni:*
a) R *è un UFD*
b) *ogni elemento irriducibile di* R *è primo.*

Dim. a)$\Rightarrow$b) Sia R un UFD e per chiarezza, per ogni classe di elementi irriducibili associati, scegliamo un rappresentante una volta per tutte e quindi rappresentiamo ogni elemento come prodotto di un certo numero di copie di tali rappresentanti per un opportuno unit.

Sia r un elemento irriducibile di R che divide il prodotto $a\ b$, cioè esista un elemento c di R tale che $a\ b = r\ c$. Essendo la fattorizzazione di a b unica, r o è un elemento della fattorizzazione di $a\ b$ oppure è associato ad uno degli irriducibili della fattorizzazione stessa: in entrambi i casi divide uno degli irriducibili di $a\ b$. D'altra parte *la fattorizzazione di* $\boldsymbol{a\ b}$ *è il prodotto delle fattorizzazioni di* $\boldsymbol{a}$ *e di* $\boldsymbol{b}$ (eventualmente a meno dell'ordine dei fattori): quindi r divide uno degli irriducibili in cui è fattorizzato a o di quelli in cui è fattorizzato b e quindi divide almeno uno dei due elementi a, b. Cioè l'irriducibile r è primo.
b)⇒a) Supponiamo che $u\ r_1\ r_2\ ....\ r_n = v\ p_1\ p_2\ ....\ p_k$ (con u e v unit) siano due diverse fattorizzazioni in irriducibili di uno stesso elemento non nullo e non unit r di R. Per ipotesi *ogni irriducibile* p_i *è primo* e quindi per l'osservazione 1.4 è associato a un fattore irriducibile r_j: quindi a meno di un cambiamento dell'ordine dei fattori, possiamo supporre che esista un unit v_1 tale che $r_1 = v_1\ p_1$. Semplificando p_1 in entrambi i membri dell'uguaglianza si trova $u\ v_1\ r_2\ ...\ r_n = v\ p_2\ ...\ p_k$. Iterando la procedura si trova che, il numero k di fattori p_i deve essere uguale al numero n di fattori r_j, e quindi gli r_j e i p_i sono a 2 a 2 associati. Ciò garantisce l'unicità della fattorizzazione. C.V.D.

Non in tutti i domini gli elementi irriducibili sono primi (e quindi non tutti i domini sono UFD): il controesempio si trova nel paragrafo 5.

PROPOSIZIONE 2.2 *Sia* R *un UFD. Per ogni coppia di suoi elementi non nulli* $\boldsymbol{a}$, $\boldsymbol{b}$ *sono definiti MCD e mcm. Inoltre, a meno del prodotto per un unit, risulta* $\mathrm{MCD}(a,b) = a\ b/\mathrm{mcm}(a,b)$.

Dim. Come nel precedente teorema fissiamo un rappresentante per ogni classe di irriducibili associati. In più decidiamo di rappresentare tramite le potenze il prodotto di più copie di uno stesso elemento irriducibile e di scrivere nella fattorizzazione dei due elementi non nulli a e b tanto i fattori di a che quelli di b, eventualmente con esponente 0: ciò serve ad avere una rappresentazione uniforme dei fattori dei due elementi ed è un artificio reso possibile dal fatto che non si fa altro che aggiungere eventualmente nella rappresentazione un unit (anzi l'unità). Siano dunque

$$a = u\ r^h\ s^k\ ...\ t^l \qquad\qquad b = v\ r^{h'}\ s^{k'}\ ...\ t^{l'}$$

Dico che $\mathrm{MCD}(a,b) = d$ ove $d = r^{\min(h,\,h')}\ s^{\min(k,\,k')}\ ...\ t^{\min(l,\,l')}$ e

$\mathrm{mcm}(a,b) = m$ ove $m = r^{\max(h,\,h')}\ s^{\max(k,\,k')}\ ...\ t^{\max(l,\,l')}$.

È chiaro che d divide a e b; d'altra parte se un altro elemento d^* divide a e b, ogni suo fattore irriducibile, essendo primo, deve dividere (vedi osservazione 1.4) qualche fattore di a e insieme qualche fattore di b e quindi d: dunque, per semplificazioni successive, si vede che d^* divide d.
Similmente m è multiplo di a e b poiché ogni fattore irriducibile dei due è in esso rappresentato alla massima potenza presente in a o in b (si proceda anche qui per semplificazioni successive). Se poi m^* è multiplo di a e di b, un fattore irriducibile che compaia in a con potenza i deve dividere m^* almeno i volte e similmente per un fattore che compaia in b: visto che la fattorizzazione è unica, m^* avrà tra i suoi fattori irriducibili tutti quelli di m, con potenza non inferiore a quella che compare in m e quindi m dividerà m^*.
Infine $(u\ v)\ d\ m = (u\ v)\ r^{\min(h,\,h') + \max(h,\,h')}\ s^{\min(k,\,k') + \max(k,\,k')}\ ...\ t^{\min(l,\,l') + \max(l,\,l')} = a\ b$. C.V.D.

Ovvia l'estensione del calcolo del MCD e del mcm allorché questi coinvolgono $n>2$ elementi. Questo metodo di calcolo è però spesso poco operativo, poiché è difficile evidenziare i fattori irriducibili di ciascun elemento. Passando dagli elementi agli ideali da essi generati, vale la

OSSERVAZIONE 2.3 *Sia* R *un* UFD e quindi siano definiti mcm e MCD.

a) $(a_1)\cap(a_2)\cap...\cap(a_n) = (\mathrm{mcm}(a_1,a_2,...,a_n))$
b) *In generale* $(a_1)+(a_2)+...+(a_n) \subseteq (\mathrm{MCD}(a_1,a_2,...,a_n))$ *ma non vale l'uguaglianza; si può usare il legame tra MCD e mcm e la formula precedente per ricostruire il MCD.*

Dim. a) Infatti, scritto per brevità m=mcm(a_1,a_2,...,a_n), si ha che m è un multiplo di ciascun a_i e quindi appartiene a $(a_1)\cap(a_2)\cap...\cap(a_n)$. D'altra parte ogni elemento che sta nell'intersezione è multiplo di ciascun a_i e quindi di m, cioè sta in (m).
b) È chiaro che d=MCD(a_1,a_2,...,a_n) divide ogni elemento $r_1a_1+r_2a_2+...+r_na_n$ di $(a_1)+(a_2)+...+(a_n)$ che quindi appartiene all'ideale generato da d. D'altra parte, in R=k[x,y] (che è un UFD, vedi §4) si ha MCD(x,y) = 1, ma (x)+(y) = (x,y) non è l'ideale (1) = R, visto che non contiene gli elementi di k.

3. PID

Ricordiamo la

DEFINIZIONE 3.1 *Un* ***ideale*** I *è detto* ***principale*** *se esiste almeno un elemento* ***s*** *di* I *che genera* I:

$$I = Rs := (s).$$

Ciò significa: $t \in (s) \Leftrightarrow s$ divide t.
Non è detto che ci sia un solo elemento s che può funzionare da generatore di I: ma se (t) = (s) si ha $t = rs$ (per qualche r in R) poiché t sta in I e, similmente, $s = r't$; da ciò, sostituendo, $t = rr't$ e, semplificando, $rr' = 1$: cioè, *i possibili generatori si ottengono uno dall'altro moltiplicando per unit*.
Ciò porta a "identificare" i possibili generatori e motiva il fatto che di solito si dica "**il**" **generatore** di I, come se fosse uno solo.

OSSERVAZIONE 3.2 *Un ideale principale è primo se e solo se è generato da un elemento primo di* R.
Infatti visto che $t \in (s) \Leftrightarrow s$ divide t, l'affermazione che definisce gli elementi primi:

se s divide $a\ b$ e non divide a, allora divide b

equivale alla

se $a\ b$ sta in (s) e a non sta in (s), allora b sta in (s)

che definisce gli ideali (principali) primi.

DEFINIZIONE 3.3 *Un* ***dominio*** R *è detto* ***a ideali principali*** (**PID**) *se ogni suo ideale* I *è principale.*

Trascurando i campi (che sono banalmente PID, contenendo solo i due ideali (0) e (1)), gli esempi più naturali di PID sono forniti da **Z** e dagli anelli di polinomi k[x] in un'indeterminata a coefficienti in un campo k. Conviene dimostrare questa asserzione in un contesto lievemente più generale.
Chiamiamo ***dominio euclideo*** *un dominio* R *in cui è possibile simulare l'algoritmo della divisione*.
Allo scopo è necessario (e sufficiente) che

1. sia definita una funzione m: R\{0}→**N**, ove **N** è l'insieme degli interi non negativi, tale che per tutte le coppie di elementi a, b di R con b non nullo si abbia $m(ab) \geq m(a)$ e che
2. per ogni coppia di elementi a, b di R con b non nullo esistano q, r in R tali che

$$a = bq + r \quad \text{e} \quad r = 0 \ \text{ oppure } \ m(r) < m(b).$$

Tanto nel caso di **Z** che in quello di k[x] queste condizioni sono realizzate; in particolare la funzione m in **Z** è il valore assoluto, mentre in k[x] è il grado (per un altro esempio vedi fine paragrafo).

OSSERVAZIONE 3.4 *Ogni dominio euclideo è un PID.*

Dim. Se I è un ideale non nullo di R, considero un elemento b di I tale che $m(b)$ sia il minimo tra gli $m(a)$ degli elementi a di I (tale minimo esiste poiché **N** è ben ordinato): mostro che I = (b).
Per ogni elemento a di I si ha $a = bq + r$ con $r = 0$ oppure $m(r) < m(b)$: visto che $r = a - bq$ appartiene ad I, non può valere la relazione $m(r) < m(b)$, in quanto violerebbe l'ipotesi di minimalità di $m(b)$ e quindi $r = 0$. C.V.D.

PROPOSIZIONE 3.5 *Sia* R *un PID. Gli ideali primi di* R *sono tutti e soli quelli generati da elementi primi di* R *e sono tutti massimali.*

Dim. Se R è un PID ogni ideale è principale e quindi si applica l'osservazione 3.2.
Inoltre, sia (p) primo: se $(p)\subseteq(s)\subseteq R$ si ha che s divide p che per ipotesi è primo e quindi irriducibile: dunque o s è un unit (e allora genera l'intero anello R) oppure è associato a p e quindi genera lo stesso ideale di p: quindi l'ideale primo (p) è massimale. C.V.D.

Ne consegue che *ogni anello quoziente di un PID o è un campo o non è un dominio di integrità*, cosa già sperimentata andando a studiare gli anelli $\mathbf{Z}_n$ di classi di resti.
Alla luce di questa proprietà si vede facilmente che

- comunque sia fatto il campo k, l'anello $k[x,y]$ dei polinomi in due indeterminate non è un PID, poiché $k[x,y]/(x) \cong k[y]$ non è un campo ma è un dominio di integrità;
- $\mathbf{Z}[x]$ non è un PID, poiché $\mathbf{Z}[x]/(x)\cong\mathbf{Z}$ non è un campo ma è un dominio di integrità (se si preferisce si può fare $\mathbf{Z}[x]/(p)\cong\mathbf{Z}_p[x]$, con p primo in $\mathbf{Z}$: di nuovo si trova un dominio che non è un campo).

Vogliamo arrivare a provare che ogni PID è un UFD: allo scopo è utile evidenziare le proprietà di divisibilità dei PID.

PROPOSIZIONE 3.6 *Sia* R *un PID.*

a) *Per ogni coppia di elementi non nulli* $\mathbf{r}$ *e* $\mathbf{s}$ *di* R *esiste* MCD(r,s)*: esso è il generatore dell'ideale* (r,s) *generato da* $\mathbf{r}$ *ed* $\mathbf{s}$. [(1)]
b) *Per ogni coppia di elementi non nulli* $\mathbf{r}$ *e* $\mathbf{s}$ *di* R *esiste* mcm(r,s)*: esso è il generatore dell'ideale* $(r)\cap(s)$.
c) *L'enunciato si estende a qualunque insieme finito di elementi di* R.

Dim. a) Sia d il generatore di (r, s): poiché r ed s appartengono all'ideale, sono multipli di d. D'altra parte, poiché d appartiene all'ideale generato da r e s, esistono r', s' in R tali che $d = rr' + ss'$ e quindi se d^* divide tanto r che s divide anche d: ne consegue che d è MCD(r,s).
b) Sia m il generatore di $(r)\cap(s)$: in quanto elemento di (r), m è un multiplo di r e per lo stesso motivo è multiplo di s. D'altra parte ogni multiplo m^* di r ed s sta nell'intersezione $(r)\cap(s)$ e quindi è multiplo del generatore m di tale ideale: ne consegue che m è mcm(r,s).
c) La dimostrazione data non dipende dal fatto di lavorare con due elementi e quindi può essere immediatamente generalizzata. c.v.d.

In particolare questo capita in $\mathbf{Z}$ e in $k[x]$.

PROPOSIZIONE 3.7 *Sia* R *un PID. Ogni elemento irriducibile* $\mathbf{r}$ *di* R *è primo.*

Dim. Se l'elemento r è irriducibile non ha divisori diversi dagli unit e dagli elementi associati a r. Quindi se r divide $a\ b$ ma non divide a, MCD(r,a) =1, cioè l'ideale (r,a) è R; in particolare esistono s, t in R tali che $1 = rs + at$ e quindi $b = r(bs) + (a\ b)t$: visto che r divide $a\ b$, r divide b. C.V.D.

LEMMA 3.8 *In ogni PID vale la condizione catenaria ascendente sugli ideali.*

Dim. Sia $I_1 \subset I_2 \subset ... \subset I_n \subset ...$ una catena ascendente di ideali di R.
La loro unione è ancora un ideale I di R, poiché due elementi di I stanno necessariamente in un ideale I_k della catena e quindi anche la loro somma, appartenendo a I_k, sta nell'unione I; similmente per il prodotto di un elemento di R per uno di I.

---

(1) Nei PID quindi la formula data nell'osservazione 2.3 vale con l'uguaglianza, cioè il MCD si lega alla somma di ideali come il mcm si lega alla loro intersezione. Val la pena di notare che a) è l'unico punto fondamentale in questo enunciato, visto che gli altri possono esser fatti discendere dall'osservazione 2.3, una volta provato che un PID è un UFD.

L'ideale I è generato da un suo elemento s: e, poiché s appartiene ad un ideale I_n della catena, risulta $I = (s) \subseteq I_n$. Poiché l'implicazione inversa vale per definizione di unione, si vede che $I = I_n$ e quindi per ogni $k > n$ si deve avere $I_k = I_n = I$. Dunque ogni catena strettamente ascendente è finita. C.V.D.

PROPOSIZIONE 3.9 *Ogni PID è un UFD.*

Dim. Visto che per la proposizione 3.7 in un PID *ogni irriducibile è primo*, per poter applicare il teorema 2.1 (di caratterizzazione degli UFD) basta mostrare che ogni un elemento non nullo e non unit r di R ammette una fattorizzazione.
Se r è irriducibile, la fattorizzazione è data da r. Sia r riducibile:

$$r = r_1\ s_1 \text{ con } r_1, s_1 \text{ non unit.}$$

Se entrambi sono irriducibili la fattorizzazione di r è trovata. Altrimenti se, ad es., r_1 è riducibile:

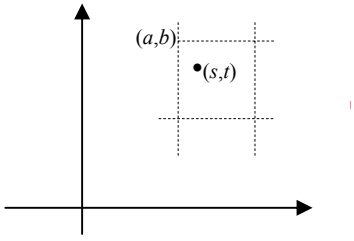
$$r_1 = r_2\ s_2 \text{ con } r_2, s_2 \text{ non unit.}$$

Se entrambi sono irriducibili la fattorizzazione di r_1 è trovata. Altrimenti se, ad es., r_2 è riducibile si itera la procedura …. Supponendo di chiamare sempre r_k l'eventuale fattore riducibile al k-esimo passaggio, si vede che $r_k | r_{k-1}$, $r_{k-1} | r_{k-2}$,..., $r_2 | r_1$ e quindi si crea una catena ascendente (strettamente, poiché tutti gli s_i sono non unit) di ideali: $(r_1) \subset (r_2) \subset ... \subset (r_k) \subset ...$ Allora per il lemma 3.8 deve esistere un n tale che $(r_n)=(r_{n+1})$. Ciò significa che $r_n = u r_{n+1}$ ove u è un unit: quindi si è trovata una fattorizzazione di r_n: procedendo a ritroso si otterrà una fattorizzazione di $r_{n-1}=r_n\ s_n$ (dopo aver eventualmente proceduto in modo simile su s_n) e così via.
Dunque una fattorizzazione si trova sempre. C.V.D.

Concludiamo questo paragrafo con un altro esempio di dominio euclideo (e quindi in particolare PID).
In $\mathbf{Z}[x]$ si consideri l'ideale I generato dal polinomio x^2+1: l'anello quoziente $\mathbf{Z}[x]/I$ è dato dall'insieme delle classi laterali $(a+bx)+I=[a+bx]$ che hanno per rappresentanti i resti dei polinomi di $\mathbf{Z}[x]$ nella divisione per x^2+1 (resti che esistono e sono unici, visto che il divisore ha coefficiente direttore invertibile in $\mathbf{Z}$). La somma è definita componente per componente: $[a+bx]+[a'+b'x] =[(a+a')+(b+b')x]$, mentre il prodotto è definito sostituendo il monomio x^2 nel polinomio prodotto dei due rappresentanti con -1: $[a+bx][a'+b'x] =[(aa'-bb')+(a'b+ab')x]$. L'anello così ottenuto è isomorfo al sottoanello del campo complesso dei numeri complessi $a+ib$ con a e b interi. Quindi è un dominio di integrità cui si dà il nome di dominio degli interi gaussiani e che si denota usualmente come $\mathbf{Z}[i]$. In tale anello il quadrato del modulo: $|a+ib|^2 =(a^2+b^2)$ ha le proprietà richieste alla funzione m: $\mathbf{Z}[i] \setminus \{0\} \to \mathbf{N}$ introdotta all'inizio del paragrafo, poiché

$$|(a+ib)(a'+ib')| = |(a+ib)|\ |(a'+ib')| > |(a+ib)|$$

se $a'+ib'$ non è nullo. Per trovare "quoziente e resto" nella divisione di un intero gaussiano α per un intero gaussiano β non nullo si considera il numero complesso $\alpha/\beta=s+it$ e si cerca l'intero gaussiano $a+ib$ tale che $|a-s| \le 1/2$ e $|b-t| \le 1/2$ (vedi illustrazione).
Allora $\alpha=(a+ib)\beta+((s-a)+i(t-b))\beta$ e risulta $|((s-a)+i(t-b))\beta|^2 \le (1/2)|\beta|^2 \le |\beta|^2$: quindi il quoziente è $a+ib$ e il resto è $((s-a)+i(t-b))\beta$.



Per qualche esercizio vedere alla fine del capitolo.

4. Ereditarietà della fattorizzazione unica.

Si vuole arrivare a dimostrare che se R è un UFD, anche R[x] lo è. Da ciò segue per ricorrenza che anche R[$x_1,\ldots,x_n$] lo è e in particolare che lo sono gli anelli di polinomi a coefficienti in un campo.
Allo scopo si dimostrerà prima che ogni elemento ha fattorizzazione e successivamente che ogni elemento irriducibile di R[x] è primo, il che in virtù del teorema 2.1 garantisce che gli elementi in R[$x_1,\ldots,x_n$] hanno fattorizzazione unica.
Per garantire l'esistenza della fattorizzazione serve il Lemma di Gauss e prima ancora un po' di terminologia.

DEFINIZIONE 4.1 *Sia* R *un UFD. Si chiamerà*

- ***contenuto*** c(f) ***di un polinomio f*** *di* R[x] *il MCD dei suoi coefficienti (che esiste essendo i coefficienti elementi dell'UFD* R*)*
- ***polinomio primitivo*** *un polinomio* f *tale che* c(f) *sia* 1.

Si ha allora, per ogni polinomio f di R[x]: f = c(f) f_1 , ove f_1 è primitivo.

LEMMA DI GAUSS *Siano* R *un UFD ed* ***f***, ***g*** *due polinomi non nulli di* R[x]. *Allora:*

i) *se* ***f*** *e* ***g*** *sono primitivi, anche* ***fg*** *lo è;*
ii) *comunque siano fatti* ***f*** *e* ***g*** , c(***fg***)=c(***f***)c(***g***).

Dim. i) Se $f = r_0 + r_1x + \ldots + r_mx^m$ e $g = s_0 + s_1x + \ldots + s_nx^n$, fg è la somma dei termini $a_i\, x^i$ i cui coefficienti a_i sono le somme dei prodotti $r_j\, s_k$ dei coefficienti di f e g tali che $j + k = i$. Se f e g sono entrambi primitivi, nessun elemento irriducibile p di R divide tutti i coefficienti di f, né tutti quelli di g: sia j il più piccolo indice tale che p non divida il coefficiente r_j di f e k il più piccolo indice tale che p non divida il coefficiente s_k di g: allora p non divide il coefficiente a_{j+k} del prodotto, poiché

$$a_{j+k} = (r_0s_{j+k} + \ldots. + r_{j-1}s_{k+1}) + r_js_k + (r_{j+1}s_{k-1} + \ldots + r_{j+k}s_0)$$

e p divide ciascuna delle due somme tra parentesi, ma non divide r_js_k (altrimenti essendo primo dividerebbe uno dei due fattori).
Dunque nessun fattore irriducibile divide contemporaneamente tutti i coefficienti del polinomio prodotto e di conseguenza il loro MCD è 1, cioè il polinomio è primitivo.
ii) Evidenziamo in ogni polinomio il contenuto: f = c(f) f_1, g = c(g) g_1, fg = c(fg) $(fg)_1$. Si ha pure fg = c(f)c(g) f_1g_1 ove f_1g_1 è primitivo visto che f_1 e g_1 sono primitivi e quindi differisce da $(fg)_1$ al più per il prodotto per un unit. Quindi, a meno del prodotto per un unit, i due coefficienti c(fg) e c(f)c(g) devono coincidere. C.V.D.

TEOREMA DI ESISTENZA *Sia* R *un UFD. Ogni polinomio non nullo di* R[x] *ha una fattorizzazione in polinomi irriducibili.*

Dim. Ogni polinomio f ha la forma f = c(f) f_1: poiché c(f) è sicuramente fattorizzabile in quanto elemento di R, basta prendere in esame il polinomio primitivo f_1. Nel seguito dimenticheremo il pedice per brevità: ricordiamo però che c(f) = 1.
Proviamo (per induzione sul suo grado) che il polinomio primitivo f può essere fattorizzato.
Se il grado è 0, f = c(f) sta in R: ovvio.
Supponiamo che ogni polinomio con grado minore di quello di f abbia fattorizzazione (ipotesi induttiva). Se il grado è >0 ed f è irriducibile non c'è nulla da provare.
Supponiamo quindi $f = g\, h$. Allora 1 = c(f) = c($g\, h$) = c(g) c(h), cioè c(g) e c(h) sono unit in R. Dunque se g avesse grado 0, coincidendo con c(g) sarebbe un unit di R e quindi di R[x], cioè f sarebbe irriducibile, contro quanto supposto. Ne segue che g (e per motivi analoghi h) deve avere grado >0 e minore del grado di f (altrimenti l'altro fattore avrebbe grado 0). Per l'ipotesi induttiva g ed h hanno una fattorizzazione in polinomi irriducibili e di conseguenza anche f, che ne è il prodotto, ne ha una. C.V.D.

Per dimostrare il teorema di unicità bisogna introdurre la nozione di *campo dei quozienti* di R.
Sia R un qualunque dominio di integrità.
In R×(R\{0}) si considerino equivalenti due coppie (r,s) ed (r',s') allorché $rs' = r's$.
Si verifica che questa è effettivamente una relazione di equivalenza: in particolare da $rs' = r's$ e $r's'' = r''s'$, si ricava $rs's'' = r'ss'' = r''s's$, e semplificando per s' – cosa possibile poiché siamo in un dominio – $rs'' = r''s$, cioè vale la proprietà transitiva.
Si dice **frazione** (o **quoziente**) r/s la classe di equivalenza che ha come rappresentante la coppia (r,s) e si denota il loro insieme con Q(R).
In Q(R) si introducano una somma e un prodotto come segue:

$$(r/s) + (p/q) = (rq + ps)/sq \qquad (r/s)\ (p/q) = rp/sq.$$

Le definizioni sono indipendenti dai rappresentanti. Infatti se $r/s = r'/s'$ e $p/q = p'/q'$:

$$(rq + ps)s'q' = rs'qq' + pq'ss' = r'sqq' + p'qss' = (r'q' + p's')sq \quad \text{e} \quad (rp)(s'q') = r'sp'q = (r'p')(sq).$$

Si verifica che per somma e prodotto valgono le proprietà commutativa ed associativa e la distributiva (basta lavorare sui rappresentanti). L'elemento neutro rispetto alla somma è $0/s$ o, equivalentemente, 0/1; similmente l'elemento neutro rispetto al prodotto è s/s cioè 1/1. L'opposto di r/s è $(-r/s)$; l'inverso di una frazione non nulla r/s è s/r.
Dunque Q(R) *è un campo*. Il sottoinsieme delle frazioni del tipo $r/1$ costituisce un sottoanello isomorfo a R (visto che $(r/1)+(p/1) = (r+p)/1$ e $(r/1)\ (p/1) = (rp)/1$): per questo si identifica $r/1$ con r.
Q(R) è detto **campo dei quozienti** di R.

TEOREMA DI UNICITÀ *Se* R *è un UFD anche* R[x] *lo è. Di conseguenza, per ogni numero naturale n, è un UFD anche il dominio* R[$x_1,\ldots, x_n$].

Dim. Visto che ogni elemento non nullo di R[x] ha almeno una fattorizzazione in polinomi irriducibili, basta provare che ogni polinomio irriducibile è primo: ciò sarebbe vero se R fosse un campo (poiché allora R[x] sarebbe un PID); la strategia di dimostrazione è allora di passare attraverso un insieme dei coefficienti che sia un campo: precisamente il campo Q dei quozienti di R.
1) *Se* f *è irriducibile in* R[x] *allora è irriducibile in* Q[x].
Sia $f = g\ h$, con g, h polinomi non nulli di Q[x]. Si scrivano i coefficienti di g in modo che abbiano tutti lo stesso denominatore $s_1 \in$ R: allora $s_1\ g = g'$ è un polinomio di R[x]; la stessa operazione su h, porta al polinomio $s_2\ h = h'$ di R[x]. Dunque

$$s_1 s_2\ f = g'\ h'$$

è un'uguaglianza in R[x]: se ne ricava, via lemma di Gauss, $c(s_1s_2)c(f) = c(g')c(h')$. Ora $c(f)=1$, poiché f essendo irriducibile è in particolare primitivo e $c(s_1s_2) = s_1s_2$. Dunque $s_1s_2 = c(g')c(h')$ e di conseguenza si possono dividere entrambi i membri dell'uguaglianza evidenziata per s_1s_2, ottenendo, se $g' = c(g')g''$ e $h' = c(h')h''$,

$$f = g''\ h''.$$

Poiché f è irriducibile, uno dei due, ad es. g'', deve essere un unit di R[x] e quindi di R: ma allora $g = g'/s_1 = (c(g')/s_1)(g''/1)$ è un elemento non nullo di Q e quindi un unit in Q[x]: cioè f è irriducibile in Q[x].
2) *Se* f *è irriducibile in* Q[x] *allora è primo in* Q[x], poiché Q[x] è un PID.
3) *Se* f *è irriducibile in* R[x] *allora è primo in* R[x].
Infatti si supponga che f divida il prodotto di polinomi $g\ h$ di R[x]. Poiché R[x] è un sottoinsieme di Q[x], f divide un prodotto di polinomi di Q[x], e poiché f è primo in Q[x] deve dividerne almeno uno: sia g. Allora esiste un polinomio g' di Q[x] tale che $g = f\ g'$. Scrivendo i coefficienti di g' in modo che abbiano tutti lo stesso denominatore s, si trova un polinomio g'' di R[x] tale che $g' = g''/s$, cioè $s\ g = f\ g''$ e, passando ai contenuti, $s\ c(g) = c(f)c(g'') = c(g'')$, poiché $c(f)=1$, visto che il polinomio è irriducibile e quindi primitivo. Allora, in R, s divide $c(g'')$ e quindi tutti i coefficienti di g'', cioè i coefficienti di g' appartengono in realtà a R: ciò significa che f divide g in R[x]. C.V.D.

Nota. Si potrebbe essere tentati di dimostrare che se f è primo in Q[x] allora è primo in R[x]…. Ma non funziona!
Ad es., se R = **Z** e quindi Q(R) = **Q**, il polinomio $6x-15$ è irriducibile e quindi primo nel PID **Q**[x], ma non è irriducibile (e quindi meno che meno può esser primo) in **Z**[x]: infatti $6x-15 = 3(2x-5)$ è la fattorizzazione in irriducibili del polinomio.

5. Un Dominio NON a Fattorizzazione Unica

In **Z**[x] si consideri l'ideale I generato dal polinomio x^2+5: l'anello quoziente **Z**[x]/I è dato dall'insieme delle classi laterali $(a+bx)+I = [a+bx]$ che hanno per rappresentanti i resti dei polinomi di **Z**[x] nella divisione per x^2+5 e può essere identificato con l'insieme $\{a+bx \mid a, b\in \mathbf{Z}, x^2 = -5\}$, in cui somma e prodotto si fanno utilizzando le ordinarie regole di commutatività, associatività e distributività e tenendo conto dell'ulteriore richiesta: $x^2 = -5$. Come già visto a proposito degli interi gaussiani, si usa indicare questo anello con **Z**[$\sqrt{(-5)}$].

Esso *è un dominio di integrità*, poiché x^2+5 è un elemento irriducibile di **Z**[x] che è un UFD – vedi teorema di unicità – e quindi è un elemento primo, cioè generatore di un ideale primo.
Per il teorema 2.1, per mostrare che **Z**[$\sqrt{(-5)}$] non è un UFD basta trovare un suo elemento irriducibile non primo [(2)].

Verifichiamo che 3 *è un elemento irriducibile non primo* di **Z**[$\sqrt{(-5)}$].
Che 3 *non* sia *primo* è immediato: 3 divide $6=(1+\sqrt{(-5)})(1-\sqrt{(-5)})$ ma non divide nessuno dei due fattori poiché, ad esempio, $1+\sqrt{(-5)} = 3(a+b\sqrt{(-5)})$ implica $3a = 1$, il che è impossibile in **Z**.
Proviamo che 3 è *irriducibile*.
Osserviamo che, se $3 = (a+b\sqrt{(-5)})(a'-b'\sqrt{(-5)})$, nessuno dei due fattori può essere nullo, altrimenti sarebbe nullo il prodotto: dunque non si può avere $a = b = 0$ né $a' = b' = 0$. Inoltre l'uguaglianza che si ottiene sviluppando: $aa'+5bb'-3 = (a'b-ab')\sqrt{(-5)}$ equivale a chiedere $ab' = a'b$ e $aa'+5bb' = 3$.
Se a, a', b, b' sono tutti non nulli, da $ab'=a'b$ si ricava che b e b' sono concordi se solo se lo sono a ed a'. Ma se deve essere $aa'+5bb'=3$, non può risultare $bb'>0$ (altrimenti $aa'+5bb'$ sarebbe non minore di 6) e neppure $bb'<0$ (in quanto la somma di due negativi non può dare 3). Dunque almeno una delle quattro coppie (a,b), (a',b'), (a,a'), (b,b') deve essere nulla: come già osservato, non può trattarsi delle prime due, né di (a,a') poiché non ci sono due numeri interi b, b' tali che $5bb'=3$. Dunque deve essere $b=b'=0$ e $aa'=3$ cioè $a=\pm 3$, $a'=\pm 1$. Ora 1 e –1 sono unit in **Z**[$\sqrt{(-5)}$] (ognuno è inverso di se stesso): poiché non si può scrivere come prodotto di due non unit, 3 risulta irriducibile.

Nota 1 In alternativa, per l'osservazione 3.2, si può dimostrare che 3 non è primo mostrando che non lo è l'ideale generato da 3 in **Z**[$\sqrt{(-5)}$]. Infatti tale ideale "coincide" con l'ideale $(3, x^2+5)/(x^2+5)$ in **Z**[x]/(x^2+5) e quindi il quoziente **Z**[$\sqrt{(-5)}$]/(3) è isomorfo a **Z**[x]/($3, x^2+5$) che, a sua volta è isomorfo a $\mathbf{Z}_3[x]/(x^2+5_3) = \mathbf{Z}_3[x]/(x^2-1_3)$ che non è un dominio di integrità visto che il suo elemento $[x-1_3]$ divide lo zero: dunque (3) non è primo in **Z**[$\sqrt{(-5)}$].

Nota 2 Nel passaggio al quoziente che porta da **Z**[x] a **Z**[$\sqrt{(-5)}$] le proprietà legate alla divisibilità non si conservano. Ad es. ci sono polinomi irriducibili come x^2+6 che si trasformano in unit, polinomi riducibili che si trasformano in unit, come $(x^2+4)(x^2+6)$; polinomi irriducibili che si trasformano in elementi riducibili, come $7+2x+x^2$.

[2)] Non è necessario mostrare che ogni elemento ammette almeno una fattorizzazione: anche se ciò fosse vero, la fattorizzazione non sarebbe unica, proprio per l'esistenza di elementi irriducibili non primi.

6. Esercizi

1) Mostrare che l'anello quoziente di $\mathbf{Z}_3[x]$ rispetto all'ideale in esso generato da x^2-2 è un campo. Quanti elementi ha? Contiene un sottocampo isomorfo a $\mathbf{Z}_3$?

2) Sia p un numero naturale primo. Mostrare che il sottoanello S_p di $\mathbf{Q}$ formato dalle frazioni che, ridotte ai minimi termini, hanno denominatore non divisibile per p è un dominio euclideo.

3) Verificare che in un PID ogni ideale si può scrivere come intersezione di un numero finito di ideali. In quale caso tali ideali sono tutti massimali?

Suggerimenti per le soluzioni

1)

- Osservare che il polinomio x^2-2 è irriducibile in $\mathbf{Z}_3[x]$ (se non lo fosse sarebbe prodotto di 2 polinomi di primo grado e quindi, per il teorema di Ruffini, un elemento di $\mathbf{Z}_3$ lo annullerebbe: verificare che non succede).
- Osservare che $\mathbf{Z}_3[x]$ è un PID e quindi x^2-2 è primo e perciò generatore di un ideale massimale. Con ciò resta provato che il quoziente è un campo.
- Gli elementi del quoziente hanno come rappresentanti polinomi di primo grado a coefficienti in $\mathbf{Z}_3$. Quindi sono 9. Provare a listarli, identificando gli elementi di $\mathbf{Z}_3$ con 0,1,2.
- È quasi ovvio che i polinomi di grado zero rappresentano elementi del campo che formano un sottocampo isomorfo a $\mathbf{Z}_3$.

2)

- Ricordare che è già stato provato che S_p è un dominio di integrità e che pS_p è il suo unico ideale massimale. Verificare che i soli ideali di S_p sono quelli della forma p^kS_p, e quindi S_p è un PID.
- Definire la funzione m: $S_p\backslash\{0\}\to\mathbf{N}$ ponendo $m(s/t)=k$ se s/t appartiene a p^kS_p ma non a $p^{k+1}S_p$. Soddisfa la condizione $m(ab)\geq m(a)$ per ogni coppia di elementi non nulli a,b di S_p?
- Definire quoziente q e resto r nella divisione di s/t per la frazione non nulla s'/t' ponendo
  se $m(s'/t') \leq m(s/t)$: $q = st'/ts'$ e $r = 0$
  se $m(s'/t') > m(s/t)$: $q =$ (quoziente nella divisione in $\mathbf{Z}$ di st' per ts') e
  $r =$ (resto nella divisione in $\mathbf{Z}$ di st' per ts')$/tt'$
  Corrisponde alla definizione di divisione data parlando di domini euclidei?

3)

- Se $I=(s)$, scrivere s come prodotto di elementi irriducibili e applicare l'osservazione 2.3.
- Applicare la proposizione 3.5.