Corso di Algebra 1

A. Machì

a. a. 2006–2007

Dispensa 4

1 Campo dei quozienti di un dominio di integrità

Ricordiamo che un dominio di integrità è un anello commutativo unitario privo di divisori dello zero. Se non si tratta di un campo, non tutti gli elementi ammettono un inverso; si può costruire allora un campo che contiene il dominio e nel quale gli elementi del dominio si invertono. La situazione è analoga a quella dell'anello degli interi, che è un dominio di integrità e nel quale, a parte 1 e –1, gli elementi non hanno inverso: si costruisce allora il campo dei razionali, che contiene gli interi, e nel quale gli interi si invertono. Il campo dei razionali è il campo delle "frazioni" o "quozienti" a/b degli interi, si construisce come insieme delle coppie (a, b) con opportune operazioni di somma e prodotto. Nel caso di un dominio di integrità il procedimento è analogo. Consideriamo l'insieme $D \times D$ delle coppie di elementi di un dominio D, con la seconda componente diversa da zero:

$$(a, b),\ a, b \in D,\ b \neq 0, \tag{1}$$

e introduciamo in questo insieme la seguente relazione:

$$(a, b)\rho(c, d) \text{ se } ad = bc.$$

Si tratta di una relazione di equivalenza:

1. Riflessiva: $(a, b)\rho(a, b)$. Vero, perchè $ab = ba$ (un dominio è commutativo.

2. Simmetrica: $(a, b)\rho(c, d)$, e dunque $ad = bc$. Ma $ad = bc$ è equivalente a $cb = da$, per la commutatività, e ciò significa $(c, d)\rho(a, b)$

3. Transitiva: $(a, b)\rho(c, d)$ e $(c, d)\rho(e, f)$ significano $ad = bc$ e $cf = de$, da cui $adf = bcf = bde$, e $(af - be)d = 0$. Ma $d \neq 0$ e la mancanza di divisori dello zero implicano $af = be$, cioè $(a, b)\rho(e, f)$.

(Si pensi ai numeri razionali, dove sono equivalenti, ad esempio, le coppie (2,3), (-2,-3), (4,6),(-4,-6), ecc., cioè le frazioni 2/3,–2/–3, 4/6).

Sia K questo insieme di classi di equivalenza, e dimostriamo che si tratta di un campo rispetto a opportune operazioni di somma e prodotto.

1. Somma. Definiamo la somma di due classi come

$$\overline{(a,b)} + \overline{(c,d)} = \overline{(ad+bc, bd)}$$

(il prodotto ab e la somma $ad+bc$ sono il prodotto e la somma di D) che ricorda la somma di due frazioni

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}.$$

Poiché abbiamo definito la somma utilizzando dei rappresentanti delle classi, occorre verificare che si tratta effettivamente di una somma tra classi, cioè che non dipende dalla scelta dei rappresentanti. Ma se scegliamo altri rappresentanti, (a',b') e (c',d'), allora $\overline{(a',b')}+\overline{(c',d')} = \overline{(a'd'+b'c', b'd')}$, e la classe risultato della somma è la stessa di prima perché $(ad+bc)b'd' = (a'd'+b'c')bd$, come si verifica sviluppando il prodotto. La somma così definita non dipende quindi dalla scelta dei rappresentanti.

2. Prodotto:

$$\overline{(a,b)(c,d)} = \overline{(ac,bd)}.$$

Intanto, La classe $\overline{(ac,bd)}$ è ancora del tipo (1) (seconda componente diversa da zero in quanto, essendo $b,d \neq 0$, anche $bd \neq 0$, per l'assenza di divisori dello zero) e quindi ha senso definire il prodotto in questo modo. Vediamo se è ben definito. Se cambiamo rappresentanti, $\overline{(a',b')(c',d')} = \overline{(a'c', b'd')}$, e questa sarà la stessa classe di prima se $acb'd' = a'c'bd$, ma questa uguaglianza è equivalente alla $ab' \cdot cd' = a'b \cdot c'd$, che è vera in quanto $ab' = cd'$ e $cd' = c'd$, per l'equivalenza tra (a,b) e (a',b'') e tra (c,d) e (c',d').

K è un gruppo commutativo rispetto alla somma:

- $\overline{(a,b)} + \overline{(c,d)} = \overline{(ad+bc,bd)} = \overline{(cb+da,db)} = \overline{(c,d)} + \overline{(a,b)}$
- la proprietà associativa si riporta a quella del dominio D;
- lo zero è la classe $\overline{(0,a)}$;
- l'opposta della classe $\overline{(a,b)}$ è la classe $\overline{(-a,b)} = \overline{(a,-b)}$ (queste due classi sono equivalenti perchè, in D, $-a \cdot -b = ab$).

K^* è un gruppo moltiplicativo:

- la classe $\overline{(a,a)}$ è l'elemento neutro 1: $\overline{(a,a)} \cdot \overline{(c,d)} = \overline{(ac,ad)} = \overline{(c,d)}$;
- per l'inverso, $\overline{(a,b)}^{-1} = \overline{(b,a)}$ (poiché la classe $\overline{(a,b)}$ è diversa dalla classe zero, cioè dalla $\overline{(0,a)}$, e la seconda componente è sempre diversa da zero, la coppia (b,a) è del tipo (1)). Si pensi alle frazioni $\frac{a}{b}$, con $a, b \neq 0$, ha come inverso $\frac{b}{a}$.

Si verifica facilmente la proprietà distributiva.

Si osservi che due coppie $(a,1)$ e $(b,1)$, $a \neq b$, non sono mai equivalenti, e dunque una coppia $(a,1)$ è l'unico elemento della propria classe: $\overline{(a,1)} = \{(a,1)\}$. Il campo K è il *campo dei quozienti* del dominio D. Nel caso in cui D è l'anello degli interi, K è il campo razionale Q:

$$Q = \{\frac{r}{s},\ r, s \in Z\};$$

nel caso un cui D è l'anello dei polinomi $F[x]$ su un campo F, K è il campo delle funzioni razionali, che si denota con $F(x)$:

$$F(x) = \{\frac{f(x)}{g(x)},\ f(x), g(x) \in F[x]\}.$$

Un campo finito F è di caratteristica $p > 0$. Lo stesso accade allora per il campo delle funzioni razionali $F(x)$ a coefficienti in F, e poiché l'unità di questo campo è la stessa di F (il campo base), abbiamo un esempio di campo infinito a caratteristica $p > 0$.

2 Omomorfismi tra anelli

Come nel caso dei gruppi, anche tra due anelli si definisce un omomorfismo. Essendoci due operazioni, si richiede che si tratti di una corrispondenza che conserva entrambe le operazioni.

Definizione. Siano A e A' due anelli. Un *omomorfismo* tra i due anelli è una corrispondenza $\varphi : A \to B$ tale che:

1. $\varphi(a+b) = \varphi(a) + \varphi(b)$;
2. $\varphi(ab) = \varphi(a)\varphi(b)$

Se φ è iniettiva e surgettiva, φ è un isomorfismo. Se φ è iniettiva, A è isomorfo a un sottoanello di B. Si dice allora che A *si immerge* in B, o che B contiene una copia di A, o semplicemente che B contiene A.

Se D è un dominio di integrità, e K il suo campo dei quozienti, la corrispondenza $D \to K$, che associa all'elemento $a \in D$ la classe $\overline{(a,1)} \in F$ è iniettiva, e inoltre conserva le due operazioni di somma e prodotto: se a $b \in D$ è associata la classe $\overline{(b,1)}$, alla somma $a+b$ è associata la classe $\overline{(a+b,1)}$, che è la somma delle due classi. E così per il prodotto.Si tratta pertanto di un isomorfismo iniettivo. Possiamo allora dire che il campo K contiene D (i razionali contengono gli interi come coppie $(a,1)$, e le funzioni razionali i polinomi come coppie $(f(x),1)$).

Sia $\varphi : R \to R'$ un omomorfismo di anelli, e sia I l'insieme degli elementi di R che vanno nello zero di R':

$$I = \{a \in R,\ \varphi(a) = 0\}.$$

I è il *nucleo* dell'omomorfismo φ. Si tratta del nucleo dell'omomorfismo φ di R in R' considerati come gruppi abeliani, e dunque I è un sottogruppo del gruppo additivo di R. Se $a \in I$ ed $r \in R$, consideriamo l'elemento ar; si ha:

$$\varphi(ar) = \varphi(a)\varphi(r) = 0 \cdot \varphi(r) = 0$$

e dunque anche $ar \in I$; analogamente, $ra \in I$. Il nucleo ha pertanto questa proprietà di *assorbimento*: se contiene un elemento a, contiene anche tutti i prodotti, a destra o a sinistra, di a per un qualunque elemento r dell'anello.

Esempi. 1. La corrispondenza $Z \to Z_n$ è un omomorfismo, di nucleo (n), l'insieme dei multipli di n.

2. Sia $Z[x]$ l'anello dei polinomi a coefficienti interi. La corrispondenza $Z[x] \to Z_n[x]$ che associa a un polinomio $f(x)$ il polinomio $\bar{f}(x)$ che ha gli stessi coefficienti presi modulo n è un omomorfismo, di nucleo i polinomi i cui coefficienti sono multipli di n.

Definizione. Sia I un sottoinsieme di un anello R (qualunque, non necessariamente di integrità o unitario) tale che:

1. rispetto alla somma, I è un sottogruppo del gruppo additivo di R;
2. se $a \in I$ ed $r \in R$, allora $aR = \{ar, r \in R\} \subseteq I$.

L'insieme I è allora un *ideale destro*. Se si richiede che $Ra = \{ra, r \in R\} \subseteq I$ si tratterà di un *ideale sinistro*. Se un ideale è insieme destro e sinistro si dirà *bilatero* (o *bilaterale*).

Esempi. 1. Nell'anello degli interi Z, l'insieme dei multipli di un fissato intero n:

$$(n) = \{kn, k \in Z\}$$

è un ideale (bilatero, perché Z è commutativo). Si tratta infatti di un sottogruppo del gruppo additivo di Z, e inoltre, moltiplicando un multiplo n per un qualunque intero si ottiene ancora un multiplo di n.

2. Nell'anello dei polinomi sopra un campo, l'insieme dei multipli di un polinomio $f(x)$,

$$(f(x)) = \{k(x)f(x),\ k(x) \in F[x]\}$$

è un ideale bilatero. La dimostrazione è la stessa del caso degli interi (ancora un'analogia tra anello degli interi e anello dei polinomi sopra un campo).

3. Nell'anello delle matrici $n \times n$ sopra un campo, le matrici "riga", cioè quelle che hanno al più una data riga, e sia la $k-$esima, non tutta nulla, formano un ideale destro I_k. Ad esempio, per I_1 (prima riga non tutta nulla) si ha:

$$\begin{pmatrix} a_1 & a_2 & \dots & a_n \\ 0 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 0 \end{pmatrix} \begin{pmatrix} x_{1,1} & x_{1,2} & \dots & x_{1,n} \\ x_{2,1} & x_{2,2} & \dots & x_{2,n} \\ \dots & \dots & \dots & \dots \\ x_{n,1} & x_{n,2} & \dots & x_{n,n} \end{pmatrix} = \begin{pmatrix} b_{1,1} & b_{1,2} & \dots & b_{1,n} \\ 0 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 0 \end{pmatrix}$$

dove $b_{1,i} = \sum_{i=1}^{n} a_1 x_{1,i}$.

Questo ideale I_1 è destro ma non sinistro:

$$\begin{pmatrix} x_{1,1} & x_{1,2} & \dots & x_{1,n} \\ x_{2,1} & x_{2,2} & \dots & x_{2,n} \\ \dots & \dots & \dots & \dots \\ x_{n,1} & x_{n,2} & \dots & x_{n,n} \end{pmatrix} \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ 0 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 0 \end{pmatrix}$$

$$= \begin{pmatrix} x_{1,1}a_1 & x_{1,1}a_2 & \dots & x_{1,n}a_n \\ x_{2,1}a_1 & x_{2,1}a_2 & \dots & x_{2,n}a_n \\ \dots & \dots & \dots & \dots \\ x_{n,1}a_1 & x_{n,1}a_2 & \dots & x_{n,n}a_n \end{pmatrix} \notin I_1,$$

e così per tutti gli I_k. Si osservi che per l'anello delle matrici $M_{n\times n}$ si ha:

$$M_{n\times n} = I_1 + I_2 + \cdots + I_n.$$

Si può verificare che le matrici "colonna" J_k formano un ideale sinistro (ma non destro), e anche in tal caso $M_{n\times n} = J_1 + J_2 + \cdots + J_n$.

L'intersezione di due ideali sinistri (destri) è un ideale sinistro (destro), e così l'intersezione di un numero qualunque di ideali. L'intersezione di un ideale sinistro e di uno destro è un ideale bilatero. Se S è un sottoinsieme

di elementi di un anello R, l'intersezione di tutti gli ideali sinistri (destri, bilateri) di R che contengono l'insieme S si chiama *ideale sinistro* (*destro, bilatero*) generato dall'insieme S, e si denota con (S). Esso costa delle somme finite di elementi di S a coefficienti nell'anello $\sum_i r_i s_i + n_i s_i$ ($\sum_i s_i r_i + n_i s_i$, $\sum_i r_i s_i r_i' + n_i s_i$ $r_i, r_i' \in R,\ n_i \in Z$). Se S consta di un solo elemento, $S = \{a\}$, allora l'ideale (a) si chiama *ideale principale generato da a.*

Esempi. 1. Nell'anello degli interi, l'ideale che consta dei multipli di un intero n è l'ideale principale generato da $S = \{n\}$.

2. Nell'anello degli interi, dato $S = \{m_1, m_2, \ldots, m_n\}$ se k è il massimo comun divisore degli m_i, l'ideale generato da S è l'ideale dei multipli di k. In particolare, se gli m_i sono primi tra loro, S genera tutto l'anello.

3. Nell'anello dei polinomi a coefficienti in un campo, i polinomi a termine noto nullo formano un ideale principale, l'ideale (x) generato dal polinomio $f(x) = x$. Infatti un polinomio a termine noto nullo $a_1x + a_2x^2 + \cdots + a_nx^n$ si può scrivere $(a_1 + a_2x + \cdots + a_{n-1}x^{n-1})x = k(x)x$, dove $k(x) = a_1 + a_2x + \cdots + a_{n-1}x^{n-1}$, e quindi come multiplo di x. Viceversa, i multipli di x sono polinomi senza termine noto: $(a_0 + a_1x + a_2x^2 + \cdots + a_nx^n)x = a_0x + a_1x^2 + a_2x^3 + \cdots + a_nx^{n+1}$.

Nell'anello $Z[x]$ dei polinomi a coefficienti interi, i polinomi a termine noto pari formano un ideale: è l'ideale generato da $S = \{2, x\}$. Infatti, i polinomi dell'ideale (S) hanno la forma $2h(x)+xk(x)$, e questi sono polinomi a termine noto pari. Viceversa, se $f(x)$ ha termine noto pari, $f(x) = 2m + a_1x + a_2x^2 + \cdots + a_nx^n$ allora $f(x) = 2m + (a_1 + a_2x^+ \cdots + a_nx^{n-1})x \in (S)$. I polinomi in cui tutti i coefficienti sono pari costituiscono l'ideale (2).

Come nel caso degli interi, polinomi relativamente primi generano tutto l'anello dei polinomi.

Teorema 1. *L'anello degli interi è un anello a ideali principali.*

Dim. Abbiamo dimostrato che un sottogruppo I di Z è ciclico, cioè è l'insieme dei multipli di un intero, $I = (n)$. Ma ogni sottogruppo di Z è anche un ideale, da cui il risultato. □

Questo risultato dipende dal fatto che nell'anello degli interi si può fare la divisione euclidea. Poiché lo stesso accade nell'anello dei polinomi, con il grado al posto dell'intero che dà il resto, abbiamo:

Teorema 2. *L'anello dei polinomi sopra un campo è un anello anello a ideali principali.*

Se R è un anello con unità 1, e I è un ideale che contiene 1, allora I coincide con tutto l'anello, $I = R$. Infatti, I conterrà allora tutti i prodotti $r \cdot 1 = r$, cioè tutti gli elementi di R.

L'anello $Z[x]$ dei polinomi a coefficienti interi, invece, non è un anello a ideali principali. Infatti, l'ideale $(2, x)$ dei polinomi a termine noto pari, visto in precedenza, non può essere principale. Se infatti $(2, x) = (f(x))$ per un certo polinomio $f(x)$, allora 2 dovrebbe essere un multiplo di $f(x)$: $2 = f(x)g(x)$, e poiché la somma dei gradi dei due polinomi è il grado della costante 2, e quindi è zero, i due polinomi hanno entrambi grado zero, cioè sono costanti: $f(x) = a, g(x) = b$, $a, b \in Z$. Allora $2 = ab$, da cui $a = \pm 1$ oppure $a = \pm 2$. Se $a = \pm 1$, $(f(x)) = (a) = (1)$ o (-1), e in entrambi i casi $(2, x) = (f(x)) = Z[x]$; ma ciò è assurdo: vorrebbe dire che tutti i polinomi hanno termine noto pari. Analogamente, se $(f(x)) = (a) = (2)$ o (-2), significherebbe che i polinomi di $(2, x)$ hanno tutti i coefficienti pari, mentre ve ne sono che hanno soltanto il termine noto pari (ad esempio, $2 + x$).

In teoria degli anelli, gli ideali bilaterali hanno il ruolo che i sottogruppi *normali* hanno in teoria dei gruppi. Sono infatti tutti e soli i nuclei degli omomorfismi, come succede ai sottogruppi normali nel caso dei gruppi. Sia I un ideale (destro o sinistro); poiché I è un sottogruppo del gruppo additivo di R, possiamo considerare le classi laterali $a+I$. Sappiamo che l'insieme R/I di queste classi è un gruppo (necessariamente abeliano) rispetto all'addizione: $(a + I) + (b + I) = a + b + I$. Se vogliamo che R/I sia un anello dobbiamo introdurre un prodotto tra queste classi. Lo definiamo come:

$$(a + I)(b + I) = ab + I, \tag{2}$$

e affinché questo prodotto sia ben definito, occorre dimostrare che se a' e b' sono altri due rappresentanti delle classi $a+bI$ e $b+I$, allora $a'b'+I = ab+I$. Ma $a' = a + i$, $b' = b + i'$ implicano $a'b' = ab + ai + i'b + i^2 \in ab + I$, in quanto $ai, i'b, i^2 \in I$ perché I è un ideale. Allora le due classi coincidono.

Nota. Il prodotto di due classi laterali di un ideale bilatero definito come nella (2) non coincide in generale con l'insieme dei prodotti degli elementi delle due classi. Si ha sempre $(a + I)(b + I) \subseteq ab + I$; infatti, con $x, y \in I$, i prodotti degli elementi delle due classi sono del tipo:

$$(a + x)(b + y) = ab + ay + xb + xy \tag{3}$$

dove $ay, xb, xy \in I$ perché I è un ideale bilatero, e la somma appartiene a I perché I è un sottoanello. Allora, $(a + x)(b + y) = ab + (ay + xb + xy) = ab + z$, con $z \in I$, per cui $(a + I)(b + I) \subseteq ab + I$. Ma l'inclusione può essere propria. Ad esempio, in

Z, se consideriamo l'ideale che consta dei multipli di 8, $I = (8)$, e la classe $4 + I$, per la definizione (2) si ha

$$(4 + I)(4 + I) = 16 + I;$$

la classe $16 + I$ contiene 24, che si ottiene come 16+8, ma 24 non si può ottenere come un prodotto di due elementi di $4 + I$, che sono tutti della forma:

$$(4 + 8h)(4 + 8k) = 16 + 32k + 32h + 64hk = 16(1 + 2k + 2h + 4hk) = 16t,$$

cioè tutti multipli di 16. L'insieme dei prodotti (3) non costituisce quindi in generale una classe, ma essendo contenuto nella classe $ab + I$, ciò basta a definire il prodotto di due classi $a + I$ e $b + I$: è la classe che contiene tutti i prodotti (3). Questa classe è individuata perché le classi sono disgiunte.

L'insieme delle classi modulo I forma un anello (le proprietà associativa e distributiva sono ovvie), l'*anello quoziente modulo l'ideale I*. Se R ha unità 1, R/I ha come unità la classe $1 + I$. Se R è commutativo, lo stesso accade per R/I. Il viceversa è ovviamente falso. Come nel caso dei gruppi, la corrispondenza $R \to R/I$ è un omomorfismo, il cui nucleo è I (verificare).

Gli ideali del quoziente sono del tipo J/I, dove J è un ideale J che contiene I. Viceversa, se J è un ideale di R, allora $(J+I)/I$ è un ideale di R/I (si vede facilmente che la somma di due ideali $J + I = \{x + y,\ x \in J, y \in I\}$ è un ideale). La situazione è analoga a quella dei gruppi.

Nell'anello degli interi Z, le classi resto modulo un intero n, Z_n, non sono altro che l'anello quoziente Z/I, dove $I = (n)$ è l'ideale che consta dei multipli di n.

È chiaro che (0) (l'insieme dei multipli di zero) e l'intero anello R sono ideali; si dicono *ideali banali*.

Lemma 1. *Un corpo ha solo ideali banali.*

Dim. Sia infatti $I \neq (0)$ un ideale di un corpo, e sia $a \in I$. Trattandosi di un corpo, a ha un inverso $a^{-1} \in R$ (per ora non necessariamente in I, ma vedremo che sta in I), ed essendo I un ideale esso contiene assieme ad a tutti i prodotti di a per un qualunque elemento dell'anello; in particolare $a \cdot a^{-1} = 1 \in I$, e pertanto $I = R$. □

È vero anche il viceversa:

Teorema 3. *Se un anello con unità R ha solo ideali (destri o sinistri) banali, allora è un corpo, e quindi, se è commutativo, un campo.*

Dim. Occorre dimostrare che dato $0 \neq a \in R$, a ammette un inverso. Consideriamo l'insieme Ra. Dimostriamo che Ra è un ideale. Ora, $ra + r'a = (r + r')a \in Ra$, $0 = 0a \in Ra$, e $-a = -1 \cdot a \in Ra$, e quindi Ra è un sottogruppo del gruppo additivo di R. Inoltre, se $b = ra \in Ra$, allora $r'b = r'ra = (r'r)a \in Ra$. Si tratta quindi di un ideale. Per ipotesi, $R = (0)$ oppure $Ra = R$. Ma $Ra \neq (0)$ in quanto $0 \neq a = 1 \cdot a \in Ra$, e pertanto $Ra = R$, e ciò significa che ogni elemento di R è del tipo ra, $r \in R$. Ma allora anche 1 ha questa forma; ne segue $ba = 1$, per un certo $b \in R$, e pertanto questo b è l'inverso di a. La stessa dimostrazione vale se si considera l'insieme aR. □

Definizione. Un ideale I di un anello R si dice *massimale*, se non esistono ideali tra I e l'anello, cioè:

$$I \subseteq J \Rightarrow I = J \text{ oppure } J = R.$$

Non è detto che un anello possegga sempre ideali massimali, e se ne esistono, ne possono esistere più d'uno. Per alcune classi di anelli essi si possono caratterizzare completamente. Ad esempio, nell'anello degli interi e in quello dei polinomi. Si ha:

Teorema 4. *Nell'anello degli interi Z, un ideale I è massimale se e solo se è l'insieme dei multipli di un numero primo p: $I = (p)$.*

Dim. Se $I = (p)$, allora I è massimale. Infatti, sia $(p) \subseteq J$. Sappiamo che $J = (n)$, l'insieme dei multipli di un certo intero n. Ne segue che anche p è multiplo di n: $p = kn$, e dunque, essendo p primo, $n = p$ oppure $n = 1$. Allora $J = (n) = (p) = I$, oppure $J = (1)$, cioè J è l'insieme dei multipli di 1, ovvero $J = R$.

Viceversa, sia $I = (n)$ massimale. Dimostriamo che n è primo. Infatti, se $n = hk$, con h, k interi positivi, allora $J = (h) \supseteq (n) = I$, e dunque $J = R$ oppure $J = I$. Se $J = R$, allora $a = 1$; se $J = I$, allora $h \in I$, e perciò $h = tn$, e quindi $n = hk = tnk$, da cui $tk = 1$, $k = 1$, $n = h$, e n è primo.

Lo stesso risultato sussiste, con la stessa dimostrazione, per l'anello dei polinomi a coefficienti in un campo $F[x]$: un ideale $I = (f(x))$ di $F[x]$ è massimale se e solo se $f(x)$ è un polinomio irriducibile.

Teorema 5. *Sia R un anello commutativo con unità, e sia I un ideale di R. Allora l'anello quoziente R/I è un campo se e solo se I è massimale.*

Dim. i) Se R/I è un campo, abbiamo visto che R/I non ha ideali non

banali, e dunque, se J/I è un ideale, si ha $J/I = R/I$, e quindi $J = R$, oppure $J/I = R/I$, cioè $J = I$. In altre parole, I è massimale.

Viceversa, se I è massimale, R/I è un anello commutativo con unità privo di ideali. Ma abbiamo visto in precedenza che allora R/I è un campo.

Ritroviamo così il fatto che se p è un numero primo, l'anello $Z/(p)$, che altro non è che Z_p, è un campo. Analogamente, se $p(x)$ è un polinomio irriducibile di $F[x]$, il quoziente $F[x]/(p(x))$ è un campo.

Esempio. L'insieme A delle funzioni reali di una variabile reale è un anello rispetto alle usuali operazioni di somma e prodotto tra funzioni. Dato un numero reale r, sia I l'insieme delle funzioni di A che si annullano su r:

$$I = \{f(x) \in R,\ f(r) = 0\}.$$

Si tratta di un ideale di A: se $f(x), g(x) \in I$, allora la somma $h(x) = f(x) + g(x)$ si annulla su r in quanto $h(r) = f(r) + g(r) = 0 + 0 = 0$; se inoltre $f(x) \in I$, allora il prodotto $f(x)k(x)$ per un qualunque elemento $k(x)$ di A si annulla su r: $f(r)k(r) = 0 \cdot k(r) = 0$. Dimostriamo che si tratta di un ideale massimale. Se $I \subset J$, sia $g(x) \in J$, $g(x) \notin I$. Allora $g(r) = s \neq 0$. Consideriamo la funzione $h(x) = g(x) - s$; questa si annulla su r in quanto $g(r) - s = s - s = 0$, e dunque appartiene a I. Pertanto la costante $s = g(x) - h(x)$ appartiene a J, e dunque anche $s \cdot s^{-1} = 1 \in J$, e così $J = A$. Ad ogni punto della retta corrisponde allora un ideale massimale: l'ideale delle funzioni che si annullano in quel punto.

Nell'anello degli interi, un numero primo p che divide un prodotto ab divide uno dei due fattori. In termini di ideali, ciò significa che se $ab \in (p)$, allora o $a \in (p)$ oppure $b \in (p)$. Siamo allora portati alla seguente definizione.

Definizione. Un ideale P di un anello commutativo con unità R si dice *primo* se $P \neq R$, e se contenendo il prodotto di due elementi dell'anello contiene uno dei due fattori:

$$ab \in P \Rightarrow a \in P \text{ oppure } b \in P.$$

Teorema 6. *Un ideale P di un anello commutativo con unità R è primo se e solo se il quoziente R/P è un dominio di integrità.*

Dim. Intanto, $P \neq R$, e dunque $1 \notin P$, per cui R/P ha un'unità $1 + P$. Se P è primo, consideriamo l'anello quoziente R/P e il prodotto di due classi

$(a+P)(b+P) = ab+P$. Se questo prodotto è la classe zero, $ab+P = P$, allora $ab \in P$, e dunque $a \in P$ oppure $b \in P$, cioè $a+P = P$, oppure $b+P = P$: una delle due classi è la classe zero. In altri termini, R/P è un dominio di integrità.

Viceversa, se R/P è un dominio di integrità, allora ammette una unità $1+P$ che non è lo zero di R/P: $1+P \neq P$ e quindi $1 \notin P$ e perciò $P \neq R$. Sia $ab \in P$; allora $(a+P)(b+P) = ab+P = P$, e poiché R/P non ha divisori dello zero, sia ha $a+P = P$, cioè $a \in P$, oppure $b+P = P$, cioè $b \in P$, e ciò significa che P è primo. □

Nell'anello dei polinomi a coefficienti interi $Z[x]$, l'insieme dei polinomi a termine noto nullo è un ideale, ed è l'ideale (x), generato dal polinomio $f(x) = x$, cioè l'insieme dei prodotti $k(x)x$ dove $k(x)$ è un qualunque polinomio di $Z[x]$. Il quoziente $Z[x]/(x) \simeq Z$ (una classe laterale modulo (x) di un polinomio è $a_0 + a_1x + \cdots + a_nx^n + (x)$. Ma $a_1x + \cdots + a_nx^n \in (x)$, e dunque la classe è la classe $a_0 + (x)$, $a_0 \in Z$. La corrispondenza $a + (x) \to a$ è un isomorfismo $Z[x]/(x) \to Z$). Il quoziente rispetto a (x) è Z che è un dominio di integrità, e dunque (x) è primo. D'altra parte, ciò si vede anche dal fatto che se il prodotto di due polinomi di $Z[x]$ è privo di termine noto, uno dei due deve essere privo di termine noto.

Poiché un campo è in particolare un dominio di integrità, dai teoremi 5 e 6 si ha che *in un anello commutativo con unità ogni ideale massimale è primo*. Il viceversa è falso. Nell'anello dei polinomi a coefficienti interi l'ideale (x) è primo ma non massimale; infatti, il quoziente $Z[x]/(x) \simeq Z$, e Z è un dominio di integrità ma non è un campo. Che non sia massimale si vede anche dal fatto che i polinomi a termine noto nullo sono particolari polinomi a termine noto pari; questi ultimi costituiscono l'ideale $(2, x) \neq Z[x]$, e si ha $(x) \subset (2, x) \subset Z[x]$. L'ideale $I = (2, x)$ è massimale: se $f(x) = a_0 + a_1x + \cdots + a_nx^n$ e a_0 è pari, allora $f(x) \in I$; se a_0 è dispari, allora $a_0 = 1 + 2k$, da cui $f(x) = 1 + (2k + a_1x + \cdots + a_nx^n) = 1 + g(x)$, dove $g(x)$ è un polinomio a termine noto pari. Il quoziente consta allora delle due classi I e $1 + I$, e pertanto è isomorfo al campo Z_2. Ne segue I massimale.

3 Relazioni

La costruzione dell'anello quoziente di una anello R (come del resto di un gruppo quoziente) ha un'importante interpretazione in termini di *relazioni* tra elementi di R. Supponiamo di eseguire le operazioni di somma e prodotto su alcuni elementi di R e di ottenere un nuovo elemento s. Se se questo

elemento s è zero, diremo che gli elementi scelti *sono legati dalla relazione* $s = 0$. Ad esempio, nell'anello degli interi Z, gli elementi 2,3 e 6 sono legati dalla relazione $2 \cdot 3 - 6 = 0$. Se $s \neq 0$, ci possiamo chiedere se è possibile modificare l'anello R in modo che $s = 0$ diventi vera. Possiamo pensare a questo procedimento come all'aggiunzione di una nuova relazione che fa crollare l'anello. Ad esempio, la relazione $3 \cdot 4 - 5 = 0$ non è vera in Z in quanto $3 \cdot 4 - 5 = 7$. Ma possiamo imporre la relazione $7 = 0$, e fare ciò significa lavorare modulo 7.

Più in generale, si possono introdurre un numero qualunque di relazioni $s_1 = 0, s_2 = 0, \ldots, s_n = 0$ e considerare l'ideale I bilaterale generato da $S = \{s_1, s_2, \ldots, s_n\}$. Il quoziente R/I va visto come l'anello ottenuto introducendo in R le n relazioni $s_1 = 0, s_2 = 0, \ldots, s_n = 0$. Poiché $s_i \in I$, le classi $s_i + I$ coincidono tutte con la classe I, cioè con la classe zero. Due elementi r ed r' di R hanno la stessa immagine in R/I se e solo se $r' - r \in I$, cioè $r' = r + r_1 s_1 + r_2 s_2 + \cdots r_n s_n$, $r_i \in R$.

Esempi. 1. Possiamo costruire formalmente il campo complesso introducendo la relazione $x^2 + 1 = 0$ nell'anello dei polinomi a coefficienti reali, cioè costruendo l'anello quoziente $F[x]/(x^2 + 1)$, dove F è il campo reale, ottenendo il campo complesso. La classe resto del polinomio $f(x) = x$ si denota di solito con i: si ha la relazione $(x+I)^2 + (1+I) = x^2 + 1 + I = I$, ovvero $i^2 + 1 = 0$.

2. Nell'anello $Z[x]$, considerare il quoziente $Z[x]/(x)$ significa considerare la relazione $x = 0$. Ma imporre $x = 0$ in un polinomio significa ridurre il polinomio al suo termine noto, che è un intero. Dunque "prendere il quoziente di $Z[x]$ rispetto all'ideale (x)" è un altro modo per dire "prendere il termine noto di ciascuno dei polinomi". Ma ogni intero è termine noto di qualche polinomio, e dunque $Z[x]/(x) \simeq Z$, come visto in precedenza.

Analogamente, $Z[x]/(x^2)$ è l'anello dei polinomi di primo grado rispetto al prodotto modulo x^2.

Considerare il quoziente $Z[x]/(2, x)$ significa porre $x = 0$, ottenendo Z, e poi $2 = 0$, ottenendo Z_2. L'ideale $(2, x^2)$ consta dei polinomi che hanno pari iltermine noteo e il coefficiente di x.

Consideriamo in $Z[x]$ la relazione $x - 1 = 0$, cioè $x = 1$. Ma ponendo $x = 1$ in un polinomio $f(x)$ si ottiene $f(1)$= somma dei coefficienti di $f(x)$, che è un intero. Ma ogni intero si può ottenere in questo modo (ad esempio, un intero n si ottiene ponendo $x = 1$ nel polinomio $f(x) = x + n - 1$). Ne segue $Z[x]/(x - 1) \simeq Z$.

Analogamente, considerare il quoziente $Z[x]/(2, x - 1)$ significa porre

$x = 1$, ottenendo Z, e poi $2 = 0$, ottenendo Z_2, che è un campo, per cui $(2, x - 1)$ è massimale.

Il quoziente $Z[x]/(6, 3x - 1)$ si ottiene imponendo le relazioni $6 = 0$ e $3x - 1 = 0$. Da quest'ultima, moltiplicando per 2, si ottiene $6x - 2 = 0$, da cui, essendo $6 = 0$, $2 = 0$. Allora $3x = x + 2x = x$ e $3x - 1 = x - 1$, e siamo nel caso precedente.

Il quoziente $Z[x]/(2x-6, 6x-15)$ si ottiene imponendo le relazioni $2x = 6$ e $6x = 15$. Moltiplicando la prima per 3 abbiamo $6x = 18$, e la seconda ora fornisce $18 = 15$, cioè $3 = 0$. Il quoziente è quindi Z_3.