Corso di Algebra 1

A. Machì

a. a. 2006–2007

Dispensa 3

1. Anelli

Un *anello* (associativo) è un insieme R dotato di due operazioni, dette somma ($+$) e prodotto ($\cdot$ tali che:

i) rispetto alla somma, R è un gruppo abeliano;

ii) rispetto al prodotto si richiede solo che sia associativo: $(ab)c = a(bc)$;

iii) le due operazioni sono legate dalle *proprietà distributive* (a destra e a sinistra): $(a+b)c = ac + bc$, $c(a+b) = ca + cb$.

La *iii*) implica che lo zero, cioè l'elemento neutro della somma, è *annullatore*, cioè:

i) $a \cdot 0 = 0 \cdot a = 0$, per ogni $a \in R$; infatti:

$$a \cdot 0 = a \cdot (b - b) = ab - ab = 0,$$

e analogamente $0 \cdot a = 0$.

ii) Inoltre, $a(-b) = -(ab)$. Occorre dimostrare che $ab + a(-b) = 0$. Ma

$$ab + a(-b) = a(b + (-b)) = a \cdot 0 = 0.$$

Analogamente, $(-a)b = -(ab)$.

iii) Si ha poi $(-a)(-b) = ab$ ("meno per meno fa più"). Infatti,

$$(-a)(-b) = -(a(-b)) = -(-(ab)) = ab,$$

(le prime due uguaglianze seguono dalla *ii*)).

Se esiste un elemento neutro rispetto al prodotto, da denotarsi con 1, l'anello si dice *unitario*. Se il prodotto è commutativo, l'anello si dice *commutativo*. Un *sottoanello* è un sottoinsieme di un anello R che sia esso stesso un anello rispetto alle stesse operazioni di R. Se gli elementi non nulli formano un gruppo, l'anello è un *corpo*. Un corpo commutativo è un *campo*. Gli usuali numeri razionali Q, reali $\mathbf{R}$ e complessi $\mathbf{C}$ sono campi. Esistono anche campi con un numero finito di elementi, ad esempio le classi resto modulo un numero primo p, Z_p (le classi diverse da zero modulo p hanno un inverso).

Esempi 1. L'esempio tipico è quello degli interi, che sono un anello commutativo unitario rispetto alle usuali operazioni di somma e prodotto.

2. I numeri pari formano un anello commutativo, non unitario, sottoanello del precedente.

3. Le classi resto modulo un intero n, Z_n, formano un anello rispetto alla somma e il prodotto modulo n. Se n non è primo, questo anello fornisce esempi di divisori dello zero. Un elemento $a \neq 0$ di un anello si dice *divisore dello zero* se esiste $b \neq 0$ tale che $ab = 0$. Se n non è primo, $n = rs$, $1 < r, s < n$, allora $[0] = [n] = [r][s]$, con $[r]$ ed $[s]$ entrambe non nulle, e sia $[r]$ che $[s]$ sono divisori dello zero.

4. Le matrici $n \times n$ a coefficienti formano un anello unitario non commutativo rispetto alla somma dei coefficienti e al prodotto righe per colonne. Anche qui esistono divisori dello zero. Ad esempio,

$$\begin{pmatrix} 1 & 1 \\ 2 & 2 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ -1 & -1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

5. Un elemento invertibile non può essere un divisore dello zero. Infatti se a ammette un inverso, e $ab = 0$, allora moltiplicando a sinistra per a^{-1} si ha:

$$a^{-1} \cdot ab = a^{-1}0 \Rightarrow b = 0.$$

In un corpo, e in particolare in un campo, ogni elemento è invertibile, e dunque un corpo non ha divisori dello zero.

2. Domini di integrità

Un *dominio di integrità* è un anello commutativo privo di divisori dello zero. Gli interi sono un dominio di integrità, come pure i campi.

Teorema 1. *Un dominio di integrità finito è un campo.*

Dim. Sia $D = \{a_1, a_2, \ldots, a_n\}$. Dimostriamo che esiste un elemento neutro, e che ogni elemento ha un inverso. Sia $a \in D$, $a \neq 0$, e consideriamo l'insieme $D' = \{a_1a, a_2a, \ldots, a_na\}$. Si tratta ovviamente di un sottoinsieme di D; dimostriamo che coincide con D. Infatti, se $a_ia = a_ja$, allora $a_ia - a_ja = 0$, da cui $(a_i - a_j)a = 0$, e poiché $a \neq 0$ e D non ha divisori dello zero, deve essere $a_i - a_j = 0$, cioè $a_i = a_j$. Ne segue $D = D'$. Allora lo stesso elemento a si trova fra quelli di D', per cui $a = a_ia$ per un certo a_i, e per la commutatività è anche $a = aa_i$. L'elemento a_i funge così da elemento neutro per l'elemento a. Dimostriamo che a_i è un elemento neutro di D (cioè è un

elemento neutro per tutti gli elementi di D). Sia $b \in D$; poiché $D = D'$, b è della forma $b = a_j a$; ne segue:

$$ba_i = (a_j a)a_i = a_j(aa_i) = a_j a = b,$$

e perciò a_i è un elemento neutro di D, $a_i = 1$. Dimostriamo che l'elemento a (che, ricordiamo, è un elemento generico) ha un inverso. Intanto, $1 \in D = D'$ è della forma $1 = a_k a$, e dunque a_k è l'inverso di a. □

3. Caratteristica di un campo

Sia F un campo, 1 l'elemento neutro di F. Sommando un certo numero di volte 1 con se stesso, $1+1+1+\cdots$ si può ottenere lo zero, oppure no. Ad esempio, se $F = Z_p$, sommando p volte 1 si ottiene 0. Se invece F è il campo razionale, reale o complesso, allora sommando 1 con se stesso quante volte si vuole non si ottiene mai 0. (Come vedremo, anche in un campo infinito può però succedere che sommando 1 un numero finito di volte si ottenga 0).

Se a è un elemento di un campo, e m è un intero, scriveremo ma per indicare la somma di m volte a:

$$ma = a + a + \cdots + a, \quad m \text{ volte.}$$

Supponiamo che in un campo, finito o infinito, $n1 = 0$ per un certo n, e sia m il più piccolo intero per cui ciò accade. Dimostriamo che m è primo. Infatti, se $m = rs$, con $r, s > 1$, allora:

$$0 = m1 = (rs)1 = (1 + 1 + \cdot + 1)(1 + 1 + \cdot + 1) = r1 \cdot s1.$$

Ma in un campo non vi sono divisori dello zero, e perciò $r1 = 0$ ovvero $s1 = 0$; in entrambi i casi si contraddice la minimalità di m. Ne segue $m = p$, primo. Questo numero primo p, che dunque è il periodo additivo dell'unità moltiplicativa 1, si chiama *caratteristica* del campo. Se invece non si ha mai che la somma di 1 un numero finito di volte è uguale a 0, allora il campo è a *caratteristica zero*. La caratteristica di un campo è dunque un numero primo o zero.

Sia ora a un qualunque elemento di F. Allora

$$pa = (1 + 1 + \cdots + 1)a = 0a = 0,$$

cioè il periodo additivo di a è p. Ne segue che in un campo tutti gli elementi hanno lo stesso periodo additivo (periodo p se la caratteristica è p, periodo infinito se la caratteristica è zero).

4. Anello dei polinomi sopra un campo

Sia F un campo, $F[x]$ l'insieme dei polinomi a coefficienti in F:

$$f(x) = a_0 + a_1 x + \cdots + a_m x^m.$$

L'intero m è il *grado* del polinomio f, e si denota con ∂f. Se $\partial f = 0$, $f(x) = a_0$ è una *costante* (un elemento del campo). Due polinomi sono uguali se hanno lo stesso grado e hanno ordinatamente uguali i coefficienti. Se $g(x) = b_0 + b_1 x + \cdots + b_n x^n$ è un altro polinomio, $n \leq m$, la *somma* dei due è il polinomio:

$$f(x)+g(x) = (a_0+b_0)+(a_1+b_1)x+\cdots+(a_n+b_n)x^n+a_{n+1}x^{n+1}+\cdots+a_m x^m,$$

che ha grado m (il più grande dei gradi dei due polinomi). Il *prodotto* è il polinomio:

$$f(x)g(x) = \sum_{k=0}^{m+n} c_k x^k,$$

dove il $k-$esimo coefficiente c_k è

$$c_k = a_k b_0 + a_{k-1} b_1 + \cdots + a_1 b_{k-1} + a_0 b_k$$

(la somma degli indici di ciascun addendo è k; gli indici degli a_i scend, quelli dei b_i salgono). Così:

$$f(x)g(x) = c_0 + c_1 x + x^2 + c_3 x^3 + \cdots + c_{n+m} x^{n+m}$$

dove

$$\begin{aligned} c_0 &= a_0 b_0, \\ c_1 &= a_1 b_0 + a_0 b_1, \\ c_2 &= a_2 b_0 + a_1 b_1 + a_0 b_2, \\ c_3 &= a_3 b_0 + a_2 b_1 + a_1 b_2 + a_0 b_3, \\ &\vdots \end{aligned}$$

ecc. $F[x]$ è un anello rispetto a queste due operazioni, come subito si verifica. Il polinomio nullo è il polinomio che ha tutti i coefficenti uguali a zero; ad esso non si attribuisce alcun grado. Per quanto visto, il grado ha queste proprietà:

i) $\partial f \geq 0$;
ii) $\partial f \leq \partial(fg) = \partial f + \partial g$.

L'anello dei polinomi ha molte proprietà in comune con l'anello degli interi. Intanto, è un anello privo di divisori dello zero, come si vede dalla definizione di prodotto. Inoltre, ed è l'aspetto più importante, esiste una divisione con resto analoga a quella degli interi.

Nel caso degli interi, dividendo a per b, si ha $a = bq + r$, con $0 \leq r < b$. Nel caso dei polinomi, una disuguaglianza analoga si ottiene utilizzando il grado ∂f del polinomio. La divisione con resto si enuncia allora come segue:

Teorema 2. *Dati due polinomi f e g, esistono due polinomi q ed r, con $\partial r < \partial g$ oppure $r = 0$ (polinomio nullo) tali che $f = qg + r$.*

Dim. Se $\partial f < \partial g$, si ha il risultato con $q = 0$ e $r = f$. Siano ora $f(x) = a_0 + a_1 x + \cdots + a_m x^m$, $g(x) = b_0 + b_1 x + \cdots + b_n x_n$ con $m \geq n$. Consideriamo

$$f_1(x) = f(x) - \frac{a_m}{b_n} x^{m-n} g(x). \tag{1}$$

Si ha $\partial f_1) \leq m - 1$; per induzione sul grado di f

$$f_1(x) = q_1(x)g(x) + r(x),$$

con $\partial r < \partial g$, oppure $r = 0$. Sostituendo questo valore di $f_1(x)$ nella (1), abbiamo:

$$f(x) - \frac{a_m}{b_n} x^{m-n} g(x) = q_1(x)g(x) + r(x),$$

cioè:

$$f(x) = \frac{a_m}{b_n} x^{m-n} g(x) + q_1(x)g(x) + r(x) = (\frac{a_m}{b_n} x^{m-n} + q_1(x))g(x) + r(x),$$

e posto $q(x) = \frac{a_m}{b_n} x^{m-n} + q_1(x)$ si ha il risultato. □

Se $r = 0$, allora g *divide* f. Come nel caso degli interi, il massimo comun divisore di due polinomi f e g è un polinomio i cui divisori esauriscono i divisori comuni di f e di g. Il Teorema 2 permette di parlare, anche nel caso dei polinomi, di *algoritmo euclideo* per la determinazione del massimo comun divisore.

5. Algoritmo euclideo

Il MCD(f,g) si determina come segue:

$f = q_1 g + r_1$; se $r_1 = 0$, MCD$(f,g) = g$. Altrimenti, $\partial(r_1) < \partial(g)$.

$g = q_2 r_1 + r_2$; se $r_2 = 0$, MCD$((f,g))$=MCD$(g, r_1) = r_1$. Altrimenti, $\partial(r_2) < \partial(r_1)$.

Si ottiene in questo modo una successione di divisioni con resto:

$$\begin{aligned}
f &= q_1 g + r_1, && \partial(r_1) < \partial(g),\\
g &= q_2 r_1 + r_2, && \partial(r_2) < \partial(r_1),\\
r_1 &= q_3 r_2 + r_3, && \partial(r_3) < \partial(r_2),\\
&\vdots\\
r_{n-3} &= q_{n-1} r_{n-2} + r_{n-1}, && \partial(r_{n-1}) < \partial(r_{n-2}),\\
r_{n-2} &= q_n r_{n-1},
\end{aligned}$$

con $r_n = 0$. Questo resto nullo si ottiene senz'altro in quanto la successione dei gradi dei resti è una successione decrescente di interi, e dunque nell'algoritmo, o si trova come resto il polinomio nullo, oppure la successione dei gradi dei resti deve necessariamente raggiungere zero, cioè si ottiene un resto che è una costante c. In quest'ultimo caso, se $r_i = q_{i+2} r_{i+1} + c$, allora al passo successivo $r_{i+1} = (r_{i+1}/c)c$, e il resto è nullo. In ogni caso, il MCD è l'ultimo resto non nullo. Se è una costante, i due polinomi sono *relativamente primi*.

Esempio.

Siano $f(x) = x^3 + 1$, $g(x) = x^2 + 1 \in Q[x]$. Si ha

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

dove $q_1 = x, r_1 = -x + 1$. Continuando,

$$x^2 + 1 = -x(-x + 1) + (x + 1)$$

dove $q_2 = -x$, $r_2 = x + 1$. Il passo successivo è:

$$-x + 1 = -1(x + 1) + 2,$$

dove $q_3 = -1$ e $r_3 = 2$. Infine,

$$x+1 = 2 \cdot \frac{1}{2}(x+1) + 0,$$

dove $q_4 = 2$ e r_4 è il polinomio nullo. Il MCD è una costante, e dunque i due polinomi sono relativamente primi.

Se invece che su Q consideriamo i due polinomi come aventi i coefficienti in Z_2, al terzo passo dell'algoritmo troviamo zero (perché 2 è zero in Z_2). In questo caso l'ultimo resto non nullo è $x+1$, che pertanto è il MCD.

Se dividiamo $5x^3+1$ per $3x^2+1$ su Q otteniamo quoziente $\frac{5}{3}x$ e resto $-\frac{5}{3}x+1$: la divisione è possibile perché, essendo Q un campo, esistono gli inversi dei coefficienti dei polinomi (si possono cioè dividere i coefficienti).

5. Fattorizzazione

Un polinomio $f(x) \in F[x]$ si dice *riducible* su F se esistono due polinomi $g(x)$ e $h(x)$, di gradi maggiori di zero, tali che $f(x) = g(x)h(x)$; $g(x)$ e $h(x)$ sono allora *fattori* di $f(x)$. Se due tali polinomi non esistono, $f(x)$ è *irriducibile* su F.

Un elemento a del campo F è una *radice* di $f(x)$ se $f(a) = 0$. Se un polinomio ha un fattore di primo grado, allora ha una radice in F: infatti, se $f(x) = (a+bx)g(x)$, allora $-a/b$ è una radice. Viceversa, se $f(x)$ ammette una radice a, allora è divisibile per $x-a$. Dividendo $f(x)$ per $x-a$, infatti, abbiamo:

$$f(x) = (x-a)q(x) + r(x),\ r(x) = 0 \text{ oppure } \delta r(x) < 1.$$

Se $r(x) = 0$, $x-a$ divide $f(x)$. Se $\delta r(x) < 1$, allora $\delta r(x) = 0$, cioè $r(x)$ è costante. Calcolando in a, abbiamo $0 = f(a) = r(a)$, cioè questa costante è zero. In ogni caso, $x-a$ divide $f(x)$. Ad esempio, con $f(x) = x^2+bx+c$, e $f(a) = 0$ abbiamo, dividendo $f(x)$ per $x-a$,

$$x^2+bx+c = (x-a)(x+a+b) + a^2+ba+c,$$

e il resto è $a^2+ba+c = f(a) = 0$.

Se un polinomio ha una radice, allora, come abbiamo visto è riducibile. Il viceversa è falso. Ad esempio, sui reali, $x^4+2x^2+1 = (x^2+1)(x^2+1)$, e dunque è riducibile, ma non ha radici. Se però è di grado al più 3, allora è riducibile se e solo se ammette una radice. In tal caso, infatti, se è riducibile, allora ha almeno un fattore di primo grado, e questo fornisce una radice.

Viceversa, se ammette una radice a, allora ha il fattore di primo grado $x - a$.

Come nel caso degli interi, anche per i polinomi esiste un teorema di fattorizzazione unica: un polinomio a coefficienti in un campo si spezza nel prodotto di polinomi irriducibili, e questa fattorizzazione è unica a meno di polinomi costanti e dell'ordine dei fattori. La dimostrazione è analoga a quella per gli interi, e si fa per induzione sul grado del polinomio f. Se $\partial f = 1$, $f = a + bx$ è irriducibile; se $\partial f > 1$, e f è riducibile, sia $f = gh$, con $\partial g < \partial f$ e $\partial h < \partial f$. Per induzione, g e h si spezzano in fattori irriducibili, e quindi anche f.

6. Costruzioni di campi

Prima di introdurre la nozione di ampliamento algebrico diamo un esempio. Consideriamo i numeri reali della forma $a + b\sqrt{2}$, con a e b razionali. Questo insieme di elementi si denota con $Q(\sqrt{2})$. Dimostriamo che questo insieme è un campo (sarà quindi un sottocampo del campo reale).

1. È chiuso rispetto alla somma, cioè la somma di due elementi della forma $a + b\sqrt{2}$ ha la stessa forma:

$$(a + b\sqrt{2}) + (c + d\sqrt{2}) = (a + c) + (b + d)\sqrt{2};$$

2. lo zero è della forma $a + b\sqrt{2}$, con $a = 0$ e $b = 0$: $0 + 0\sqrt{2}$;
3. l'opposto di $a + b\sqrt{2}$ ha la stessa forma: $(-a) + (-b)\sqrt{2}$.

Ne segue che $Q(\sqrt{2})$ è un gruppo abeliano rispetto alla somma. Dimostriamo che gli elementi non nulli formano un gruppo rispetto al prodotto.

1. Chiusura:

$$(a + b\sqrt{2})(c + d\sqrt{2}) = (ac + 2bd) + (ad + bd)\sqrt{2}.$$

2. Esiste un elemento neutro 1: $1 + 0\sqrt{2}$.

3. Ogni elemento diverso da zero ha un inverso (si tratta del procedimento noto come "razionalizzazione del denominatore"). Intanto, l'inverso esiste in R perché R è un campo; scriviamolo come $\frac{1}{a+b\sqrt{2}}$, e dimostriamo che si può ridurre alla forma $x + y\sqrt{2}$. Moltiplichiamo $\frac{1}{a+b\sqrt{2}}$ sopra e sotto per $a - b\sqrt{2}$:

$$\frac{1}{a + b\sqrt{2}} \cdot \frac{a - b\sqrt{2}}{a - b\sqrt{2}} = \frac{a - b\sqrt{2}}{a^2 - 2b^2} = \frac{a}{a^2 - 2b^2} + \frac{-b}{a^2 - 2b^2}\sqrt{2}$$

che è della forma $x + y\sqrt{2}$.

Ne segue che $Q(\sqrt{2})^*$ è un gruppo, e pertanto $Q(\sqrt{2})$ è un campo. È chiaro che gli argomenti ora esposti si possono usare per tutti gli elementi del tipo $a + b\sqrt{m}$, dove m è un qualunque intero che non sia un quadrato.

Il numero $\sqrt{2}$ è un numero reale, radice del polinomio $x^2 - 2$ a coefficienti razionali. Su Q questo polinomio non ha radici. Se supponiamo di conoscere solo Q, come costruire una radice di $x^2 - 2$ o,più precisamente, un campo in cui $x^2 - 2$ abbia una radice?

L'idea è la seguente, e come vedremo è applicabile a tutti i campi e a tutti i polinomi irriducibili. Per fissare le idee, consideriamo ancora $x^2 - 2$. Intanto, non bisogna guardare al solo polinomio $x^2 - 2$, ma considerare *tutti i polinomi a coefficienti razionali*, cioè l'insieme $Q[x]$. In seguito, considerare le classi resto modulo il polinomio $x^2 - 2$, cioè l'insieme quoziente modulo $x^2 - 2$, che denotiamo con $Q[x]/(x^2 - 2)$. Come rappresentanti di queste classi si possono allora prendere i polinomi di $Q[x]$ di grado 0 e 1, che costituiscono i possibili resti della divisione per un polinomio di secondo grado: gli elementi della classe $a + bx$ hanno la forma $a + bx + h(x)(x^2 - 2)$. La somma tra classi, e il prodotto tra classi definito modulo $x^2 - 2$, danno a questo insieme struttura di campo. L'esistenza dell'inverso di una classe è garantita dal fatto che $x^2 - 2$ è irriducibile, e dunque $a + bx$ e $x^2 - 2$ sono relativamente primi, per cui esistono (Bézout) $h(x)$ e $k(x)$ tali che $(a + bx)h(x) + (x^2 - 2)k(x) = 1$. Modulo $x^2 - 2$, questa uguaglianza diventa $[a + bx][c + dx] \equiv 1 \bmod (x^2 - 2)$, dove $c + dx$ è la classe di $h(x)$ modulo $x^2 - 2$. Le altre proprietà delle operazioni di somma e prodotto sono ovvie. (È evidente l'analogia con le classi resto degli interi modulo un numero primo).

Posto $F = \frac{Q[x]}{(x^2-2)}$, consideriamo i polinomi $F[y]$ sul campo F, e tra questi il polinomio $y^2 - \overline{2}$ (la classe $\overline{2}$ è la classe $2 + k(x)(x^2 - 2)$, cioè la classe dei polinomi della forma 2 + un multiplo di $x^2 - 2$).

L'elemento $\overline{x}$, cioè la classe cui appartiene il polinomio x, *è una radice di* $y^2 - \overline{2}$. Infatti, sostituendo $\overline{x}$ a y si ha $\overline{x}^2 - \overline{2}$, e questa differenza è la classe $\overline{x^2 - 2}$, cioè la classe 0, che è lo zero di F. E poiché il quadrato della classe $\overline{x}$ è la classe $\overline{2}$, possiamo dire che la classe $\overline{x}$ è la "radice quadrata" della classe $\overline{2}$.

Gli elementi $a + b\sqrt{2}$ considerati in precedenza sono allora in realtà le classi $a + bx$ modulo $x^2 - 2$, rappresentate come polinomi grado al più 1 nella "variabile" $\sqrt{2}$.

Il campo $Q(\sqrt{2})$ si dice *ampliamento* o *estensione* di Q mediante $\sqrt{2}$. Pensando a Q e a $\sqrt{2}$ immersi nei reali, $Q(\sqrt{2})$, se un sottocampo dei reali contiene Q e $\sqrt{2}$, contiene tutti i prodotti di un numero razionale con $\sqrt{2}$,

e quindi anche la somma di questi prodotti con un qualunque razionale. Contiene cioè tutti gli elementi della forma $a + b\sqrt{2}$. Un sottocampo dei reali che contiene Q e $\sqrt{2}$ contiene $Q(\sqrt{2})$; in questo senso, $Q(\sqrt{2})$ è il più piccolo sottocampo di R che contiene Q e $\sqrt{2}$.

Il discorso è generale. Sia $p(x)$ un polinomio irriducibile su un campo F, e consideriamo le classi resto dell'anello $F[x]$ modulo $p(x)$, che denotiamo con $F[x]/(p(x))$. Questo insieme è un campo:

1. $[f] + [g] = [f + g]$. Questa somma è ben definita: se si cambiano i rappresentanti,

$$[f + hp] + [g + kp] = [f + g + (h + kp] = [f + g].$$

2. La classe $[0]$ è la classe $[p(x)]$ dei multipli del polinomio $p(x)$.

3. L'opposta della classe in cui sta il polinomio f è la classe in cui sta $-f$: $-[f] = [-f]$.

Si tratta dunque di un gruppo rispetto alla somma. Vediamo il prodotto.

1. $[f][g] = [fg]$, e anche questa operazione è ben definita.

2. Se $[f] \neq [0]$, cioè f non è un multiplo di $p(x)$, allora per l'irriducibilità di $p(x)$ si ha $(f(x), p(x)) = 1$, e al solito da $h(x)f(x) + k(x)p(x) = 1$ si ha la classe $[h(x)]$ come inversa della $[f(x)]$.

Pertanto, $F[x]/(p(x))$ è un campo. I suoi elementi si possono identificare con i polinomi di grado $< \partial p(x)$ a coefficienti in F (come nel caso di $x^2 - 2$, si tratta in realtà dei polinomi di grado $< \partial p(x)$ a coefficienti nel campo $K = F[x]/(p(x))$ nella radice $\overline{x}$ del polinomio $p(y) \in K[y]$).

Esempi. 1. Il campo dei numeri complessi si ottiene come quoziente dell'anello dei polinomi a coefficienti reali $R[x]$ modulo il polinomio $x^2 + 1$. La classe $\overline{x}$ si denota di solito con i, e i numeri complessi sono i polinomi di primo grado in i: $a + bi$.

2. Consideriamo $x^3 - 5$. Le classi resto modulo questo polinomio sono rappresentate dai polinomi di grado < 3,

$$a + b\sqrt[3]{5} + c(\sqrt[3]{5})^2,\ a, b, c \in Q.$$

Come nel caso degli interi, nel quale le classi resto modulo n sono un campo se e solo se n è primo, le classi resto modulo un polinomio $p(x)$ sono un campo se e solo se $p(x)$ è irriducibile. Se infatti $p(x)$ è riducibile, $p(x) = h(x)k(x)$, con $h(x)$ e $k(x)$ di grado > 0, allora $\overline{0} = \overline{p(x)} = \overline{h(x)}\ \overline{k(x)}$, e poiché $h(x)$ e

$k(x)$ sono di grado minore del grado di $p(x)$ nessuna delle due può essere la classe 0.

7. Costruzione di campi finiti

Conosciamo il campo Z_p; a partire da questo vogliamo ora costruire altri campi finiti. Sia $p(x)$ un polinomio di $Z_p[x]$ irriducibile su Z_p, il campo $K = Z_p[x]/(p(x))$ costruito nel precedente paragrafo sarà anch'esso finito, perché consta dei polinomi di grado $< \partial p(x)$ che sono in numero finito.

Esempio. In $Z_2[x]$, e consideriamo il polinomio $p(x) = x^2 + x + 1$. Questo polinomio è irriducibile su Z_2 (è di secondo grado e non ha radici in Z_2), e dunque $Z_2[x]/(p(x))$ è un campo. Esso consta dei polinomi di grado < 2, cioè di grado 0 (le costanti) e di grado 1, che sono:

$$0, 1, x, x + 1.$$

Il prodotto del campo è il prodotto modulo x^2+x+1. La tavola del prodotto è la seguente:

	1	x	$x+1$
1	1	x	$x+1$
x	x	$x+1$	1
$x+1$	$x+1$	1	x

Ad esempio, poiché $x^2 + x + 1 \equiv 0$, e quindi $x^2 + x \equiv 1$, si ha $x(x+1) = x^2 + x \equiv 1$. Analogamente, $x\dot{x} = x^2 \equiv x + 1$. Si osservi che rispetto al prodotto gli elementi non nulli formano un gruppo, che avendo ordine 3 è necessariamente ciclico: $x, x^2 = x + 1, x^3 = x \cdot x^2 = x(x + 1) = x^2 + x \equiv 1$.

Abbiamo così il campo con 4 elementi $K = \{0, 1, x, x+1\}$. Si osservi che non può trattarsi delle classi resto modulo 4, in quanto queste non formano un campo, ma solo un anello.

Analogamente, possiamo costruire un campo con 8 elementi, a partire da un polinomio irriducibile di terzo grado su Z_2, ad esempio $x^3 + x + 1$, che è irriducibile (è di terzo grado e non ha radici in Z_2). I polinomi di grado < 3 su Z_2 sono:

$$0, 1, x, x + 1, x^2, x + 1, x^2 + x, x^2 + x + 1,$$

e questi formano un campo con il prodotto modulo $x^3 + x + 1$. Il gruppo moltiplicativo ha 7 elementi, e dunque è ciclico. Avendo ordine primo, ogni elemento è un generatore; ad esempio, x è un generatore:

x,
x^2,
$x^3 = x + 1$,
$x^4 = x(x + 1) = x^2 + x$,
$x^5 = x \cdot x^4 = x(x^2 + x) = x^3 + x^2 = x^2 + x + 1$ $(x^3 + x + 1 \equiv 0 \Rightarrow x^3 \equiv x + 1)$,
$x^6 = x^5 \cdot x = x^3 + x^2 + x = x + 1 + x^2 + x = x^2 + 1$,
$x^7 = x(x^2 + 1) = x^3 + x = 1$.

Questo campo ha 8 elementi (ma non si tratta di Z_8, che non è un campo).

Per ogni numero primo p, e ogni intero n, possiamo costruire un campo con p^n elementi come segue: si considera l'anello $Z_p[x]$, un polinomio $p(x)$ di grado n irriducibile su Z_p[1], e l'insieme dei polinomi di $Z_p[x]$ di grado $< n$. Questi ultimi sono in numero di p^n. Infatti, essi si ottengono scegliendo in tutti i modi possibili n coefficenti per formare un tale polinomio:

$$a_0 + a_1 x + a_2 x^2 + \cdots + a_{n-1} x^{n-1}.$$

Abbiamo p scelte per a_0, p per a_1,..., p per a_{n-1}: in tutto $p \cdot p \cdot p \cdots p$, n volte, e dunque p^n scelte. Ognuna di queste scelte fornisce un polinomio di grado $< n$. Con il prodotto modulo $p(x)$ abbiamo il campo richiesto.

7. Ampliamenti algebrici

Sia K un campo, F un suo sottocampo, $F \subseteq K$. Allora K è uno spazio vettoriale su F con F campo degli scalari: i vettori sono gli elementi di K, la somma tra vettori è la somma del campo K, e il prodotto di uno scalare $a \in F$ per un elemento k di K è il prodotto ak come definito in K (poiché $F \subset K$, a è anche un elemento di K). Come ogni spazio vettoriale, allora, K ha una base su F, cioè un insieme di elementi di K tali che ogni elemento di K si scrive in modo unico come combinazione lineare finita di elementi di B a coefficienti in F. Se la base B è finita, $B = \{b_1, b_2, \ldots, b_n\}$ allora ogni $k \in K$ si scrive come $k = a_1 b_1 + a_2 b_2 + \cdots + a_n b_n$, $a_i \in F$. L'unicità della scrittura significa che gli elementi di una base sono *linearmente indipendenti*, cioè che nessuno è combinazione lineare degli altri, e ciò è equivalente a dire che una combinazione lineare di elementi di una base è zero se, e solo se, tutti i coefficienti di questa combinazione sono zero. Si dimostra che in uno spazio vettoriale tutte le basi hanno la stessa cardinalità. Questa comune cardinalità è la *dimensione* dello spazio. In uno spazio di dimensione finita n, $n + 1$ vettori sono sempre dipendenti.

[1] Si può dimostrare che per ogni p ed n, esiste un polinomio di grado n irriducibile su Z_p.

Esempi. 1. Il campo $Q(\sqrt{2})$ è uno spazio vettoriale su Q di dimensione 2: $B = \{1, \sqrt{2})\}$. Infatti, ogni elemento di $Q(\sqrt{2})$ è del tipo $a + b\sqrt{2}$, e dunque del tipo $a \cdot 1 + b \cdot \sqrt{2}$. I due elementi 1 e $\sqrt{2}$ sono indipendenti, Se infatti $a \cdot 1 + b \cdot \sqrt{2} = 0$ per certi $a, b \in Q$, si avrebbe $\sqrt{2} = -\frac{a}{b}$, e $\sqrt{2}$ sarebbe razionale, assurdo.

2. Il campo complesso è uno spazio vettoriale sui reali di dimensione 2. Una base è data da $B = \{1, i\}$. Un numero complesso ha infatti la forma $a \cdot 1 + b \cdot i$, con a e b reali.

3. Il campo con 8 elementi visto nel § 7 è di dimensione 3, una base essendo data dai tre polinomi $1, x, x^2$. Ogni polinomio del campo si scrive infatti come $a \cdot 1 + b \cdot x + c \cdot x^2$.

4. In generale, un anello di polinomi $F[x]$ su un campo F è uno spazio vettoriale su F di dimensione infinita; una base è data dagli infiniti monomi $B = \{1, x, x^2, x^3, \ldots\}$. Per un fissato n, i polinomi di grado $\leq n$ formano un sottospazio (sono chiusi rispetto alla somma e al prodotto per un elemento di F).

Un elemento di K si dice *algebrico su* F se è radice di un polinomio a coefficenti in F. Ad esempio, con $F = Q$ e $K = R$, $\sqrt{2}$ è un elemento di R che è radice del polinomio $x^2 - 2$ i cui coefficienti 1 e 2 appartengono a Q: pertanto, $\sqrt{2}$ è algebrico su Q. Un elemento di K che non è algebrico su F si dice *trascendente su* F. Ad esempio, i numeri π ed e sono numeri reali trascendenti sui razionali (esiste una infinità non numerabile di numeri reali trascendenti sui razionali).

Ogni elemento di un campo K è algebrico sul campo stesso: se $a \in K$, a è radice di $x - a$, un polinomio i cui coefficienti sono 1 e a, entrambi elementi di K.

Il campo $Q(\sqrt{2})$ visto nel § 6 è un campo che contiene Q: si dice allora che è un *ampliamento di* Q *ottenuto aggiungendo* $\sqrt{2}$, e poiché $\sqrt{2}$ è algebrico su Q si dice che l'ampliamento è *algebrico*.

Teorema. *Se K è un campo ampliamento del campo F, e se, come spazio vettoriale, K ha dimensione finita su F, allora ogni elemento di K è algebrico su F.*

Dim. Sia n la dimensione di K su F, e sia $a \in K$. Allora gli $n+1$ elementi $1, a, a^2, \ldots, a^n$ sono dipendenti su F, cioè una loro combinazione lineare a

coefficienti in F non tutti nulli è zero:

$$a_0 + a_1 a + a_2 a^2 + \cdots + a_n a^n = 0,\ a_i \in F.$$

Ma allora a è radice del polinomio $a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$, e pertanto è algebrico. □