ALGEBRA COMPUTAZIONALE

Capitolo I. TERMINOLOGIA

Lo scopo di queste pagine è di richiamare le nozioni algebriche che verranno usate nel corso, illustrandole con qualche esempio di riferimento.
Le dimostrazioni, ove presenti, si intendono inserite come esercizio per lo studente, per abituarlo al ragionamento deduttivo. In prima lettura possono tranquillamente essere saltate e riprese semmai quando successivi esempi o enunciati stimolino la curiosità di vedere perché le cose funzionino in un certo modo.

1. ALCUNE STRUTTURE ALGEBRICHE

Nel corso saremo soprattutto interessati ad **anelli**, **domini** e **campi**.
Partiamo però qualche passo prima, in modo da avere un linguaggio completo.

DEFINIZIONE 1.1 *Siano* S *un insieme e* $*$ *un'operazione binaria. Diremo che*

i) (S,$*$) *è un* ***semigruppo*** *se l'operazione è associativa, cioè per ogni terna di elementi* $\boldsymbol{r}$, $\boldsymbol{s}$, $\boldsymbol{t}$ *di* S *risulta:* $(\boldsymbol{r}*\boldsymbol{s})*\boldsymbol{t}=\boldsymbol{r}*(\boldsymbol{s}*\boldsymbol{t})$

ii) (S,$*$) *è un* ***monoide*** *se è un semigruppo ed esiste un elemento* $\boldsymbol{e}$ *di* S *neutro rispetto all'operazione, cioè tale che per ogni* $\boldsymbol{s}\in$ S *risulti:* $\boldsymbol{s}*\boldsymbol{e} = \boldsymbol{s} = \boldsymbol{e}*\boldsymbol{s}$

iii) (S,$*$) *è un* ***gruppo*** *se è un monoide e per ogni* $\boldsymbol{s}\in$ S *esiste un elemento* $\boldsymbol{s}'$ *tale che:* $\boldsymbol{s}*\boldsymbol{s}'=\boldsymbol{e}=\boldsymbol{s}'*\boldsymbol{s}$

iv) (S,$*$) *è un* ***gruppo abeliano*** *se* (S,$*$) *è un gruppo e l'operazione è commutativa, cioè per ogni coppia di elementi* $\boldsymbol{s}$, $\boldsymbol{t}\in$ S *risulti:* $\boldsymbol{s}*\boldsymbol{t} = \boldsymbol{t}*\boldsymbol{s}$.

Nella terminologia dei gruppi, l'operazione è pensata come un prodotto e quindi l'elemento neutro è pensato come un'unità e di conseguenza l'elemento s' è chiamato inverso e denotato con s^{-1}. Se però l'operazione è una somma, conviene chiamare zero l'elemento neutro e opposto l'elemento s', denotandoli rispettivamente con 0 e $-s$.

ESEMPI 1.2 Si denoti con $\mathbf{Z}$ l'insieme di tutti i numeri interi relativi, $2\mathbf{Z}$ l'insieme dei numeri pari, $\mathcal{M}_n(\mathbf{R})$ l'insieme delle matrici quadrate di ordine n a coefficienti reali, $GL_n(\mathbf{R})$ il suo sottoinsieme formato dalle matrici quadrate invertibili. Si indichi con \ la differenza insiemistica. Si verifichi che:

a) $(2\mathbf{Z}\setminus\{0\},)$, dove è il prodotto tra interi, è un semigruppo che non è un monoide
b) $(\mathbf{Z}\setminus\{0\},)$ è un monoide commutativo (cioè in cui l'operazione è commutativa)
c) $(\mathcal{M}_n(\mathbf{R})\setminus\{\mathbf{0}\},)$ se è il prodotto tra matrici e $\mathbf{0}$ è la matrice nulla è un monoide non commutativo
d) $(GL_n(\mathbf{R}),)$ è un gruppo non abeliano
e) $(\mathbf{Z},+)$, dove + è l'operazione di somma tra interi, è un gruppo abeliano
f) $(\mathcal{M}_n(\mathbf{R}),+)$, dove + è la somma tra matrici, è un gruppo abeliano.

NOTA 1.3 In realtà, per verificare che (S,$*$) è un gruppo basta meno di quanto richiesto dalla definizione. Infatti si dimostra che se $*$ è associativa ed

- esiste un elemento e di S tale che per ogni $s\in$ S risulti: $s*e = s$
- per ogni $s\in$ S esiste un elemento s' (chiamiamolo inverso destro di s) tale che: $s*s' = e$

allora si ha anche $s'*s = e$ (ove s' è l'inverso destro di s) ed $e*s = s$ (anche se sembra strano, la dimostrazione si fa proprio in quest'ordine: vedi esercizio 1).
Inoltre si dimostra (ed è importante ricordare) che

- in un monoide (S,$*$) l'elemento neutro e è unico
- in un gruppo (S,$*$), per ogni elemento s, l'inverso (destro e sinistro per quanto appena visto) è unico.

DEFINIZIONE 1.4 *Siano*: R *un insieme,* $+$ *e* $\cdot$ *due operazioni binarie, tra coppie di elementi di* R, *che chiameremo somma e prodotto. Diremo che*

i) (R,+, $\cdot$) *è un* ***anello*** *se* (R,+) *è un gruppo abeliano con elemento neutro* 0, (R\{0}, $\cdot$) *è un monoide e le due operazioni sono legate dalle proprietà distributive, cioè per ogni terna di elementi* $\boldsymbol{r}, \boldsymbol{s}, \boldsymbol{t} \in$ R *si ha* $\boldsymbol{r}\cdot(\boldsymbol{s}+\boldsymbol{t}) = \boldsymbol{r}\cdot\boldsymbol{s}+\boldsymbol{r}\cdot\boldsymbol{t}$ *e* $(\boldsymbol{r}+\boldsymbol{s})\cdot\boldsymbol{t} = \boldsymbol{r}\cdot\boldsymbol{t}+\boldsymbol{s}\cdot\boldsymbol{t}$

ii) (R,+, $\cdot$) *è un* ***anello commutativo*** *se è un anello e il prodotto è commutativo*

iii) (R,+, $\cdot$) *è un* ***dominio di integrità*** *se è un anello commutativo e il prodotto di due elementi non nulli è non nullo*

iv) (R,+, $\cdot$) *è un* ***campo*** *se* (R\{0}, $\cdot$) *è un gruppo abeliano.*

OSSERVAZIONI 1.5

a) Ciò che abbiamo definito anello è in realtà un **anello con unità** (rispetto al prodotto si chiede che sia un monoide): visto che gli esempi più significativi di anelli hanno unità e che nel seguito ci interesseranno solo anelli commutativi con unità, non è sembrato utile allungarne il nome.

b) Ci sono anelli non commutativi: l'esempio più noto è dato da $(\mathbf{M}_n(\mathbf{R}),+,\cdot)$. In questo caso lo zero è la matrice nulla, l'unità è la matrice identica.

c) Le proprietà distributive garantiscono che *in ogni anello* $r\cdot 0 = 0\cdot r = 0$, *comunque si scelga* r.

d) Da ciò, sempre per le proprietà distributive, si deduce che $r\cdot(-1) = -r = (-1)\cdot r$

e) Ma, anche se $r\cdot 0 = 0 = 0\cdot r$, non è vero che in ogni anello valga la cosiddetta **proprietà di annullamento del prodotto** che definisce i domini di integrità. Ad esempio l'insieme $\mathbf{Z_4}$ delle classi di resto[1] modulo 4, con le operazioni indotte dalle operazioni sugli interi è un anello commutativo ma si ha $[2]_4\cdot[2]_4 = [0]_4$ (in quanto $4\equiv 0 \bmod 4$). In quali altri anelli di classi di resto si verifica la stessa situazione?

f) Sia R un anello che non è un dominio di integrità. Chiameremo **divisore dello zero** ogni elemento non nullo $r\in$R tale che esista un elemento non nullo $s\in$R (non necessariamente distinto da r) per cui r s=0: ovviamente anche s è un divisore dello zero.

g) *In ogni dominio di integrità valgono le* ordinarie ***regole di cancellazione***. Infatti $r\cdot t = s\cdot t$ implica $0 = r\cdot t - s\cdot t = (r-s)\cdot t$ e quindi, non essendoci divisori dello zero, se $t \neq 0$ risulta $r-s = 0$, cioè $r = s$. Anzi la validità delle regole di cancellazione è equivalente alla mancanza di divisori dello zero.

h) *Ogni campo è un dominio di integrità*: infatti, visto che ogni elemento non nullo r ha inverso r^{-1}, da $r\cdot s = 0$ si ricava $r^{-1}\cdot r\cdot s = r^{-1}\cdot 0$, cioè $s = 0$.

i) Non è in generale vero il viceversa: ad es. $(\mathbf{Z},+,\cdot)$ è un dominio di integrità che non è un campo, poiché gli elementi diversi da ± 1 non hanno inverso intero. Similmente vedremo che anche i polinomi a coefficienti in un dominio di integrità (in particolare in un campo) sono domini di integrità, ma non campi poiché i polinomi di grado >0 sicuramente non hanno inverso nell'insieme dei polinomi.

j) Però *ogni dominio di integrità* R *con un numero finito di elementi è un campo*. Infatti detti $r_1,\ldots, r_n$ gli elementi non nulli di R, i prodotti $r_1\cdot r_k, \ldots, r_n\cdot r_k$ sono tutti distinti (in quanto, valendo le regole di cancellazione, da $r_i\cdot r_k = r_j\cdot r_k$ si ricava $r_i = r_j$), non nulli e quindi opportunamente riordinati coincidono con $r_1, \ldots, r_n$; in particolare uno di questi prodotti coincide con 1 e quindi, per ogni k, l'elemento r_k ha inverso.

k) Ben noti esempi di campi infiniti sono quelli dei numeri razionali, reali, complessi, con le ordinarie operazioni. Si provi a dimostrare che le classi di resto modulo un numero primo p danno luogo a un campo finito (eventualmente si veda l'appendice).

2. SOTTOSTRUTTURE DEGLI ANELLI

Visti i nostri interessi successivi, d'ora in poi (R,+, $\cdot$) denoterà sempre un anello commutativo (con unità 1).

[1] Per una definizione e qualche proprietà generale degli anelli di classi di resto vedi appendice finale.

DEFINIZIONE 2.1 *Un sottoinsieme non vuoto* S *di un anello* (R,+,) *che rispetto alle stesse operazioni risulta a sua volta un anello (con unità!) sarà detto* ***sottoanello*** *di* R.

Per verificare che S è un sottoanello di (R,+,) basta verificare che:
- S contiene l'unità di R
- per ogni coppia di elementi $s, s' \in S$ anche $s - s' \in S$
- per ogni coppia di elementi $s, s' \in S$ anche $s\ s' \in S$

Perché?

ESEMPI e OSSERVAZIONI 2.2
a) L'insieme {0} costituito dal solo zero dell'anello R non è un sottoanello di R poiché non contiene l'unità di R. Invece, se serve, R può essere pensato come sottoanello di sé stesso.
b) $2\mathbf{Z}$ non è un sottoanello di $\mathbf{Z}$, poiché 1 non è un numero pari.
c) $\mathbf{Z}$ è un sottoanello del campo $\mathbf{Q}$ dei numeri razionali.
d) È noto che i numeri razionali possono essere rappresentati da frazioni e sotto quali condizioni due frazioni rappresentano lo stesso numero razionale. Consideriamo dunque il sottoinsieme S_p del campo $\mathbf{Q}$ formato da quei numeri razionali che, rappresentati come frazioni ridotte ai minimi termini, hanno il denominatore che non è divisibile per un certo numero primo p. Si verifichi che S_p è un sottoanello di $\mathbf{Q}$, ma che non tutti i suoi elementi non nulli hanno inverso. Si spieghi perché S_p è comunque un dominio di integrità.
e) Vedremo che ogni anello R è un sottoanello dell'anello dei polinomi in una indeterminata a coefficienti in R.
f) L'unità di S coincide con quella di R. Dunque *se* $\boldsymbol{s}$ *ha inverso in* S *ha* (lo stesso) *inverso anche in* R. Si mostri con un esempio che non è vero il viceversa.
g) *L'intersezione di un famiglia* (anche non finita) *di sottoanelli di* R *è un sottoanello* di R.

DEFINIZIONE 2.3 *Un sottoinsieme non vuoto* I *di un anello* (R,+,) *è detto* ***ideale*** *di* I *se* (I,+) *è un gruppo e per ogni* $\boldsymbol{i} \in$ I *e ogni* $\boldsymbol{r} \in$ R *risulta* $\boldsymbol{i}\ \boldsymbol{r} \in$ I.
Si usa descrivere più brevemente l'ultima proprietà scrivendo: $IR \subseteq I$. Per la commutatività del prodotto, ciò equivale a chiedere $RI \subseteq R$.

Per verificare che I è un ideale di (R,+,) basta verificare che:
- I non è vuoto (ad es. contenga lo zero di R)
- per ogni coppia di elementi $i, i' \in I$ anche $i + i' \in I$
- per ogni $r \in R$ e ogni $i \in I$ anche $r\ i \in I$.

Perché?

ESEMPI e OSSERVAZIONI 2.4
a) Comunque sia fatto l'anello R, l'insieme {0} ed R sono ideali di R. Per questo sono detti **ideali banali**.
b) Per ogni intero n, $n\mathbf{Z}$ è un ideale di $\mathbf{Z}$. Più in generale:
c) *Per ogni elemento a di* R *l'insieme* aR$=\{a\ r, r \in$ R$\}$ *è un ideale di* R.
d) Non tutti gli ideali di cui al punto (c) sono distinti: ad esempio aR$=(-a)$R, anche se $2a \neq 0$.
e) *Se* R *è un campo non ha ideali non banali*: infatti se I è un ideale non nullo contiene un elemento invertibile: a. Ma allora $1 = a\ a^{-1}$ sta in I e quindi per ogni $r \in$ R si ha $r = 1\ r \in$ I cioè I=R.
f) *Se* R *non ha ideali non banali è un campo* [(2)]. Infatti in tal caso, aR o coincide con {0} (ma allora $a\ 1 = 0$ e quindi $a = 0$) oppure coincide con R. Allora esiste un $r \in$ R tale che $a\ r = 1$, cioè a ha inverso.

[2)] Attenzione: anche se non esplicitamente, qui **gioca l'ipotesi di commutatività** del prodotto (che permette di definire gli ideali in modo semplice). Ci sono anelli non commutativi, come quello delle matrici, che non hanno ideali bilateri eppure hanno elementi non nulli che non hanno inverso.

g) Come si vede dalla dimostrazione fatta in (e) *un ideale proprio non può contenere elementi invertibili di* R, *né l'unità di* R.
h) In particolare *un ideale proprio non sarà mai un sottoanello* e viceversa *un sottoanello proprio non sarà mai un ideale* [3].
i) *L'intersezione di un famiglia* (anche non finita) *di ideali di* R *è un ideale di* R.
j) *L'intersezione tra un ideale* I *ed un sottoanello* S *di* R *è un ideale di* S.

Si è già visto che un modo per trovare un ideale di un anello è quello di evidenziarne un elemento. Precisiamo l'idea con la seguente

DEFINIZIONE 2.5 *Sia* A *un sottoinsieme* (anche non finito) *di* R. *Si dice* ***ideale generato da*** A *il più piccolo ideale di* R *che contiene* A. *Gli elementi dell'insieme* A *si chiamano* ***generatori*** [4] ***dell'ideale***. *Se un ideale ha almeno un insieme finito di generatori si dice che l'****ideale*** *è* ***finitamente generato***.

L'ideale generato da A è (per definizione) l'intersezione di tutti gli ideali che contengono A. È ovvio che in tali ideali devono stare tutte le somme finite del tipo $a_1\, r_1+\ldots+a_n\, r_n$, ove n varia in $\mathbf{N}$, gli elementi a_k variano in A e gli elementi r_k in R ($1 \le k \le n$). D'altra parte si verifica facilmente che l'insieme AR di queste somme è un ideale di R, per cui l'ideale generato da A è proprio

$$\mathrm{AR}=\{a_1\, r_1 + \ldots + a_n\, r_n \mid n\in\mathbf{N},\ r_k\in\mathrm{R},\ a_k\in\mathrm{A},\ 1\le k\le n\}.$$

In particolare:

- se A è formato da un solo elemento a si parla di ***ideale principale generato da*** a. Esso è l'ideale $a\mathrm{R}=\{a\, r,\ r\in\mathrm{R}\}$ già visto nell'esempio 2.4 (c). Quando è chiaro in quale anello si lavora tale ideale è denotato con (a)
- se $\mathrm{A}=\{a_1, \ldots, a_n\}$ è finito ed è chiaro in quale anello si lavora si usa denotare l'ideale AR generato da A con $(a_1, \ldots, a_n)$.

ESEMPI 2.6
a) Se I è un ideale di R, un insieme di generatori di I è dato da tutto I: ovviamente è un insieme di generatori di scarsa utilità pratica.
b) Nell'anello $\mathbf{Z}$ si consideri $\mathrm{A}=\{6,10\}$. Si verifichi che l'ideale generato da A è $2\mathbf{Z}$. In generale, se $\mathrm{A} = \{m, n\}$ qual è l'ideale generato da A in $\mathbf{Z}$? E se A è un insieme finito di interi?
c) Si verifichi che $p\mathrm{S}_p$ è un ideale proprio del sottoanello S_p di $\mathbf{Q}$. Come sono gli elementi di S_p che non stanno in $p\mathrm{S}_p$? Come sono fatti gli altri ideali propri di S_p? Che intersezione hanno con $p\mathrm{S}_p$?

La nozione di insieme di generatori di un ideale permette di introdurre una nuova operazione tra ideali: la somma.

DEFINIZIONE 2.7 *Siano* I *e* J *due ideali di* R. *L'****ideale*** I + J ***somma*** *di* I *e* J *è l'ideale generato da* $\mathrm{I}\cup\mathrm{J}$. Esso consiste degli elementi di R aventi la forma $i + j$, con $i\in\mathrm{I}$ e $j\in\mathrm{J}$. In maniera analoga si definisce la somma di un numero finito di ideali.

ESEMPI 2.8
a) Mostrare che $2\mathbf{Z} + 3\mathbf{Z} = \mathbf{Z}$. In generale come è fatto l'ideale $m\mathbf{Z} + n\mathbf{Z}$?
b) Se $a_1,\ldots,a_n$ sono elementi di R, si ha $a_1\mathrm{R} + \ldots + a_n\mathrm{R} = (a_1, \ldots, a_n)$. Questo è il motivo per cui qualche volta si usa la scrittura $a_1\mathrm{R} + \ldots + a_n\mathrm{R}$ per indicare l'ideale generato da $\{a_1, \ldots, a_n\}$.

---

[3] In realtà sottoanelli e ideali giuocano due ruoli "complementari", come vedremo parlando di omomorfismi di anelli.

[4] Spesso un insieme dei generatori di un ideale viene anche detto **base** dell'ideale: al contrario di quanto succede negli spazi vettoriali questo non sottintende nessuna idea di minimalità.

3. OMOMORFISMI DI ANELLI

DEFINIZIONE 3.1 *Sia* φ: R$\to$S *un'applicazione tra due anelli* $(R,+_R, \ _R)$ *con unità* 1_R *e* $(S,+_S, \ _S)$ *con unità* 1_S. *Si dice che* φ *è un* ***omomorfismo di anelli*** *se valgono le seguenti condizioni:*

- $\varphi(\boldsymbol{a} +_R \boldsymbol{b}) = \varphi(\boldsymbol{a}) +_S \varphi(\boldsymbol{b})$ *per tutte le coppie di elementi* $\boldsymbol{a}$, $\boldsymbol{b}$ *di* R
- $\varphi(\boldsymbol{a} \ _R \boldsymbol{b}) = \varphi(\boldsymbol{a}) \ _S \varphi(\boldsymbol{b})$ *per tutte le coppie di elementi* $\boldsymbol{a}$, $\boldsymbol{b}$ *di* R
- $\varphi(1_R)=1_S$.

La definizione è faticosa per via di tutti quegli indici $_R$, $_S$ che servono solo a rendere evidente che a sinistra del simbolo di uguaglianza consideriamo operazioni in R, a destra operazioni in S. Di solito si trascurano gli indici:

- $\varphi(\boldsymbol{a} + \boldsymbol{b}) = \varphi(\boldsymbol{a}) + \varphi(\boldsymbol{b})$ *per tutte le coppie di elementi* $\boldsymbol{a}$, $\boldsymbol{b}$ *di* R
- $\varphi(\boldsymbol{a} \ \boldsymbol{b}) = \varphi(\boldsymbol{a}) \ \varphi(\boldsymbol{b})$ *per tutte le coppie di elementi* $\boldsymbol{a}$, $\boldsymbol{b}$ *di* R
- $\varphi(1)=1$

e questo mette in evidenza che φ "conserva le operazioni", come si suol dire, cioè copia (in maniera più o meno fedele) la struttura che c'è in R nell'immagine φ(R).
Ovviamente la copia è più fedele quando φ è un'applicazione biunivoca: in questo caso si parla di **isomorfismo** e, dal punto di vista algebrico, i due anelli possono essere identificati.

OSSERVAZIONI 3.2

a) Se φ: R$\to$S è un omomorfismo di anelli si ha: $\varphi(0)=0$ e $\varphi(-r)= -\varphi(r)$, per ogni $r\in$ R.
b) La composizione di due omomorfismi di anelli φ: R$\to$S e ψ: S$\to$T è un omomorfismo di anelli $\psi\circ\varphi$: R$\to$T.
c) Se φ: R$\to$S è un isomorfismo di anelli, anche φ^{-1}: S$\to$R è un isomorfismo di anelli.
d) L'immagine φ(R) è un sottoanello di S.
e) L'insieme $\{r\in R \mid \varphi(r)=0\}$ è un ideale di R. Esso è detto **nucleo di** φ ed è spesso denotato con $\ker(\varphi)$.
f) Se φ è un isomorfismo o comunque un omomorfismo iniettivo, $\ker(\varphi)=(0)$, poiché l'immagine di un elemento diverso da 0 deve essere diversa da 0. Se invece l'omomorfismo non è iniettivo esistono elementi distinti a, b di R tali che $\varphi(a) = \varphi(b)$ e quindi $a-b\in\ker(\varphi)$. Viceversa tutti gli elementi di R che si ottengono sommando ad a un elemento del nucleo sono trasformati da φ nello stesso elemento $\varphi(a)$. Quindi più il nucleo di un omomorfismo è grande e più sono "numerosi" gli elementi di R trasformati nello stesso elemento. In questo senso si dice che il nucleo di φ misura quanto l'omomorfismo è lontano dall'essere un isomorfismo.

ESEMPI 3.3

a) L'identità ι: R $\to$ R definita da $\iota(r) = r$ è un isomorfismo di anelli.
b) φ: R $\to$ R definita da $\varphi(r) = -r$ **non** è un isomorfismo di anelli, a meno che per ogni $r\in$ R sia $r = -r$. Infatti $\varphi(1) = -1 \neq 1$.
c) L'applicazione φ: $\mathbf{C} \to \mathbf{C}$ definita da $\varphi(r) = \overline{r}$ (coniugato di r) è un isomorfismo di anelli.
d) L'applicazione φ: $\mathbf{Z} \to \mathbf{Z}$ definita da $\varphi(r) = 2r$ non è un omomorfismo di anelli, poiché $\varphi(1)=2$.
e) L'applicazione φ: $\mathbf{Z} \to \mathbf{Z}_2$ [5] definita da $\varphi(r) = [r]_2$ è un omomorfismo di anelli con nucleo $2\mathbf{Z}$.
f) In generale è un omomorfismo l'applicazione φ: $\mathbf{Z} \to$ R definita ponendo $\varphi(z) = z\cdot 1_R$. Esso può avere nucleo nullo (come succede se R=$\mathbf{Q}$) oppure no (come succede nel caso precedente).
g) Altri esempi potrebbero essere costruiti a partire da anelli di polinomi, di cui però non abbiamo ancora parlato. Val la pena di ricordare qui che, indicato con $\mathbf{R}[x]$ l'anello dei polinomi sul campo reale, l'applicazione φ: $\mathbf{R}[x] \to \mathbf{C}$ definita da $\varphi(1) = 1$ e $\varphi(x) = i$ (unità immaginaria) ed estendendo la definizione in modo che siano conservati somma e prodotto è un omomorfismo.

[5] Con $\mathbf{Z_2}$ si denota l'anello delle classi di resto modulo 2, cioè i pari e i dispari con l'ordinaria aritmetica (la somma di un pari e di un dispari è dispari, le altre somme sono sempre pari; il prodotto di due dispari è dispari, gli altri prodotti sono sempre pari). Con $[r]_2$ si denota la classe di resto cui appartiene r.

4. ANELLO QUOZIENTE. TEOREMA DI OMOMORFISMO

È venuto il momento di correlare ideali, sottoanelli e omomorfismi di anello.

DEFINIZIONE 4.1 *Siano* I *un ideale di un anello* R *ed* ***a*** *un elemento di* R. *Chiamiamo* (***classe***) ***laterale di*** I ***mediante a*** *il seguente sottoinsieme di* R

$$a + \mathrm{I} = \{a + i \mid i \in \mathrm{I}\}.$$

In inglese questi sottoinsiemi si chiamano **coset** o **residue class** (cioè classe di resto) **modulo I**. Forse quest'ultima terminologia meglio delle altre spiega che le classi laterali si costruiscono mimando quel che si fa costruendo le classi di resto nella divisione tra interi.
Un esempio di classe laterale l'abbiamo appena incontrato parlando di omomorfismi: l'insieme degli elementi di R che vengono trasformati da φ in φ(a) è proprio il laterale a + ker(φ) di a mediante ker(φ).

OSSERVAZIONI 4.2

a) I = 0+I è un laterale;
b) ogni elemento $a \in$ R appartiene ad un laterale mediante I;
c) $a + \mathrm{I} = b + \mathrm{I} \Leftrightarrow a - b \in \mathrm{I}$;
d) se $c \in (a + \mathrm{I}) \cap (b + \mathrm{I})$, esistono $i, i' \in \mathrm{I}$ tali che $c = a+i = b+i' \Rightarrow a-b = i'-i \in \mathrm{I} \Rightarrow a + \mathrm{I} = b + \mathrm{I}$;
e) se $a-b \notin \mathrm{I}$, $(a + \mathrm{I}) \cap (b + \mathrm{I}) = \varnothing$.

Da queste osservazioni si deduce che i laterali mediante I costituiscono una **partizione di** R e come rappresentante del laterale si può prendere uno qualsiasi dei suoi elementi (si sceglie il più semplice, se c'è qualche criterio per giudicare della semplicità dell'elemento).

ESEMPIO 4.3 In **Z** si consideri I=6**Z.** Quanti sono i suoi laterali? Cominciamo ad elencarli: I, 1+I, 2+I, 3+I, 4+I, 5+I: questi sono tutti distinti, poiché la differenza di due rappresentanti non sta mai in I. Non ce ne sono altri poiché ogni numero intero a si può scrivere come $6q + r$ (con $0 \le r < 6$) e quindi a+I = r+I. Ovviamente posso rappresentare 5+I anche come 47+I, ma questo non rende più semplice la rappresentazione; oppure come −1+I e questo può essere un modo interessante e talora più semplice di vedere il laterale 5+I [6].

Dire che i laterali costituiscono una partizione di R significa che possiamo introdurre una relazione $\Re$ di equivalenza tra gli elementi di R: $a \Re b \Leftrightarrow a-b \in$ I ed "identificare" gli elementi che stanno nella stessa classe di equivalenza [7].

Nell'insieme dei laterali *introduciamo due operazioni* in questo modo:

- somma: (a+I) + (b+I) = (a+b) + I
- prodotto: (a+I)(b+I) = (ab) + I

Grazie al fatto che I è un ideale, il risultato di queste operazioni *non dipende dai rappresentanti* scelti per individuare i laterali a+I e b+I.
Ad esempio, se $a' = a+i$ e $b' = b+j$ (con $i, j \in$ I) si ha per definizione

$$(a'+\mathrm{I})(b'+\mathrm{I}) = (a'b') + \mathrm{I} = [ab+(aj+ib+ij)] + \mathrm{I} = (ab) + \mathrm{I}$$

poiché $a'b' - ab = aj+ib+ij \in$ I.

---

6) Val la pena di osservare che questo corrisponde a due modi di intendere il resto nella divisione tra interi: si può volere sempre un resto positivo, ancorché grande oppure preferire (per problemi di ragionevole arrotondamento) un resto negativo, ma di valore assoluto più piccolo.

7) È quel che facciamo quando parliamo di numeri pari o dispari, trattandoli come un tutt'uno, senza preoccuparci delle proprietà che possono rendere ad es. un numero dispari molto diverso da un altro (si pensi ad es. all'essere primo).

DEFINIZIONE 4.4 *L'insieme dei laterali con queste due operazioni è un anello commutativo con unità* 1+I (*e zero* I): *esso viene detto* ***anello quoziente di*** R ***rispetto a*** I *e viene denotato con* R/I

ESEMPIO 4.5 Costruiamo l'anello quoziente di $\mathbf{Z}/3\mathbf{Z}$. I suoi elementi sono i laterali $3\mathbf{Z}=[0]$, $1+3\mathbf{Z}=[1]$, $2+3\mathbf{Z}=-1+3\mathbf{Z}=[-1]$ e le operazioni sono illustrate dalle seguenti due tabelle

+	[0]	[1]	[−1]
[0]	[0]	[1]	[−1]
[1]	[1]	[−1]	[0]
[−1]	[−1]	[0]	[1]

Azione degli elementi neutri evidenziata in giallo

×	[0]	[1]	[−1]
[0]	[0]	[0]	[0]
[1]	[0]	[1]	[−1]
[−1]	[0]	[−1]	[1]

Tra parentesi, si nota che $\mathbf{Z}/3\mathbf{Z}$ è un campo.

Abbiamo denotato i laterali di $\mathbf{Z}/3\mathbf{Z}$ con lo stesso simbolo adottato altrove per le classi di resto. Ciò ha senso, poiché vedremo che $\mathbf{Z}/3\mathbf{Z}$ è isomorfo a $\mathbf{Z}_3$ (vedi teorema di omomorfismo).
Innanzi tutto, vale il seguente

TEOREMA 4.6 *Se* I *è un ideale proprio di* R *l'applicazione* γ: R → R/I *definita ponendo*

$$\gamma(r) = r + \mathrm{I} \quad \textit{per ogni } r \in \mathrm{R}$$

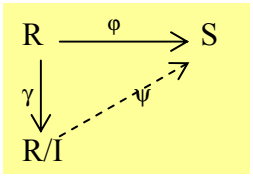
è un omomorfismo suriettivo di anelli, di nucleo $\ker(\gamma) = \mathrm{I}$. *Esso è detto* ***omomorfismo canonico*** *da* R *a* R/I [8].

Ricordiamo che, se φ: R→S è un omomorfismo, $\varphi(a)=\varphi(b)$ se (e solo se) $a-b \in \ker(\varphi)$, in particolare se $a-b$ sta in un ideale I contenuto in $\ker(\varphi)$. Ciò suggerisce che, per ogni ideale $\mathrm{I} \subseteq \ker(\varphi)$ si può vedere l'omomorfismo φ come composizione di due omomorfismi. Questo è il senso del

TEOREMA DI OMOMORFISMO *Siano* φ: R→S *un omomorfismo di anelli e* I *un ideale di* R *contenuto in* $\ker(\varphi)$. *Sia inoltre* γ: R→R/I *l'omomorfismo canonico. Allora l'applicazione* ψ: R/I→S *definita ponendo*

$$\psi(r+\mathrm{I}) = \varphi(r) \textit{ per ogni } r \in \mathrm{R}$$

i) *è ben definita (cioè non dipende dal rappresentante scelto per il laterale)*
ii) *è un omomorfismo di anelli*
iii) *si ha* $\psi \circ \gamma = \varphi$, cioè si può spezzare φ come illustrato nel diagramma a lato.



In particolare, se $\mathrm{I} = \ker(\varphi)$, vale il

COROLLARIO 4.7 *Siano* φ: R→S *un omomorfismo di anelli. Allora l'omomorfismo definito ponendo* $\psi(r+\ker(\varphi)) = \varphi(r)$ *è un isomorfismo di anelli tra* R/I *e* φ(R).

Tornando all'esempio 4.5, si ha che
l'applicazione φ: $\mathbf{Z}\to\mathbf{Z}_3$ definita da $\varphi(n)=[n]_3$ è un omomorfismo suriettivo di nucleo $3\mathbf{Z}$ e quindi, per il corollario 4.7, $\mathbf{Z}/3\mathbf{Z}$ è isomorfo a $\mathbf{Z}_3$: nella pratica confondo gli elementi dei due anelli.

Talora si usa questo corollario per studiare l'anello quoziente R/I riconducendolo ad un anello noto S che sia immagine di R tramite un omomorfismo φ avente nucleo I.
Ad esempio: l'insieme $\mathbf{R}^X$ delle funzioni definite su un insieme $X \subseteq \mathbf{R}$ a valori reali è un anello rispetto alla somma e al prodotto definiti puntualmente: $(f+g)(x)=f(x)+g(x)$, $(fg)(x)=f(x)g(x)$, per tutti gli x di X. L'insieme I di tali funzioni che hanno valore nullo in un punto fissato $x_0 \in$ X è un ideale di $\mathbf{R}^X$. Chi è l'anello $\mathbf{R}^X/\mathrm{I}$? Conviene considerare l'applicazione φ: $\mathbf{R}^X \to \mathbf{R}$ definita da $\varphi(f)=f(x_0)$. Si verifica che è un omomorfismo suriettivo con $\ker(\varphi)=\mathrm{I}$: quindi $\mathbf{R}^X/\mathrm{I}$ è isomorfo a $\mathbf{R}$.

[8] La verifica è lasciata al lettore.

Ci sono altri due teoremi che conviene aver presente quando si parla di anelli quozienti.

1° TEOREMA DI ISOMORFISMO *Siano* R *un anello,* S *un suo sottoanello,* I *un ideale proprio di* R. *Allora*

i) $S\cap I$ *è un ideale di* S

ii) $S+I=\{s+i \mid s\in S, i\in I\}$ *è un sottoanello di* R *e* I *è un ideale* di S+I

iii) *Gli anelli quozienti* $S/(S\cap I)$ e $(S+I)/I$ *sono isomorfi nell'isomorfismo che associa all'elemento* $s+(S\cap I)$ *di* $S/(S\cap I)$ *l'elemento* $s+I$ *di* $(S+I)/I$.

Si lascia la verifica al lettore. Per il terzo punto si osservi che l'omomorfismo $\varphi: S \to (S+I)/I$ definito ponendo, per ogni $s\in S$, $\varphi(s) = s+I$ ha nucleo $S\cap I$ e si utilizzi il corollario 4.7.

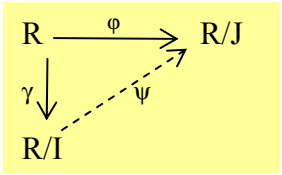
Tenuto conto che se $\varphi: R\to S$ è un omomorfismo di anelli

- l'immagine di ogni ideale di R è un ideale di $\varphi(R)$ [9]
- l'insieme $\varphi^{-1}(I')$ degli elementi a di R tali che $\varphi(a)$ appartiene ad un ideale I' di S è un ideale di R che contiene $\ker(\varphi)$,

si arriva a provare il

2° TEOREMA DI ISOMORFISMO *Siano* R *un anello,* I *e* J *due ideali propri di* R *con* $I\subseteq J$. *Allora* R/J *è isomorfo a* $(R/I)/(J/I)$.

La dimostrazione è un'applicazione del corollario 4.7 con diagramma a lato, pur di osservare che $\ker(\psi) = J/I$.



ESEMPIO 4.8 Siano $S = \mathbf{Z}/12\mathbf{Z}$ e $\varphi: \mathbf{Z}\to\mathbf{Z}/12\mathbf{Z}$ l'omomorfismo canonico.
Allora $\varphi(n\mathbf{Z})=(n\mathbf{Z}+12\mathbf{Z})/12\mathbf{Z}$ è un ideale di $\mathbf{Z}/12\mathbf{Z}$ che

- coincide con l'anello $\mathbf{Z}/12\mathbf{Z}$ se n e 12 sono primi tra loro,
- con lo zero ($12\mathbf{Z}$) se 12 divide n
- negli altri casi coincide con $d\mathbf{Z}/12\mathbf{Z}$, ove d è il massimo comun divisore tra 12 e n.

Ciò evidenzia, oltre a quelli banali, gli ideali $2\mathbf{Z}/12\mathbf{Z}$, $3\mathbf{Z}/12\mathbf{Z}$, $4\mathbf{Z}/12\mathbf{Z}$, $6\mathbf{Z}/12\mathbf{Z}$.
Il 2° teorema di isomorfismo dice che, ad esempio, $(\mathbf{Z}/12\mathbf{Z})/(4\mathbf{Z}/12\mathbf{Z})$ è isomorfo a $\mathbf{Z}/4\mathbf{Z}$.

Gli esercizi 3, 4 in fondo al capitolo illustrano ulteriormente alcuni temi di questo paragrafo.

Attenzione: si consiglia una lettura approfondita dei quattro paragrafi che seguono ed in special modo del 6 e del 7 che non si limitano a fornire il lessico necessario per il corso ma ne costituiscono il punto di partenza.

[9] Se l'omomorfismo in esame è quello canonico, $\varphi: R\to R/J$, l'immagine di un ideale I di R ha la forma $(I+J)/J$.

5. IDEALI MASSIMALI ED IDEALI PRIMI

DEFINIZIONE 5.1 *Sia* M *un ideale proprio dell'anello* R. *Si dice che* M *è un ideale massimale se per ogni ideale* I *con* $M \subseteq I \subseteq R$ *si ha* M=I *oppure* I=R.

Detto brevemente: non ci sono ideali tra M e R.
Ad esempio sono massimali in **Z** gli ideali $p\mathbf{Z}$ con p numero primo.

OSSERVAZIONE 5.2 M *è un ideale massimale di* R *se e solo se* R/M *è un campo*.
Infatti sia M massimale: se a è un elemento di R che non sta in M (e quindi tale che a+M non è lo zero di R/M), l'ideale aR+M non coincide con M e quindi coincide con R. In particolare 1 appartiene a aR + M e quindi esistono $r \in$ R ed $m \in$ M tali che $1 = ar+m$, cioè $1-ar \in$ M. Ciò significa che $(a+M)(r+M)=1+M$, cioè ogni elemento non nullo di R/M è invertibile.
Viceversa, sia R/M un campo. Se $M \subseteq I \subseteq R$, I/M è un ideale di R/M e quindi o è l'ideale nullo ($\Rightarrow$I=M) oppure è l'intero anello quoziente ($\Rightarrow$I=R): dunque M è massimale.

Il lemma di Zorn (nella forma del principio della catena) permette di mostrare che
Ogni anello con unità ha almeno un ideale massimale.

Quindi se a è un elemento non invertibile di R ($\Rightarrow a\mathrm{R} \neq \mathrm{R}$), in R/$a$R c'è un ideale massimale che avrà la forma M/aR (con M ideale di R che contiene aR): si verifichi che M è massimale in R, cioè vale la

OSSERVAZIONE 5.3 *Ogni elemento non invertibile di* R *è contenuto in un ideale massimale*.

DEFINIZIONE 5.4 *Sia* P *un ideale proprio dell'anello* R. *Si dice che* P *è un ideale primo se* $rs \in$ P *implica che almeno uno dei due elementi* r, s *appartiene a* P.

Detto diversamente,

$$\text{P è primo} \iff rs \in \mathrm{P} \text{ e } r \notin \mathrm{P} \text{ implicano } s \in \mathrm{P}$$

o anche

$$\text{P è primo} \iff r \notin \mathrm{P} \text{ e } s \notin \mathrm{P} \text{ implicano } rs \notin \mathrm{P}$$

Ad esempio in **Z** l'ideale 3**Z** è primo, invece l'ideale 6**Z** non lo è poiché ad esempio 2 3 appartiene a 6**Z**, ma né 2, né 3 appartengono a 6**Z**.

OSSERVAZIONE 5.5 P *è un ideale primo di* R *se e solo se* R/P *è un dominio di integrità*.
Infatti

- $(r+\mathrm{P})(s+\mathrm{P}) = \mathrm{P}$ e $(r+\mathrm{P}) \neq \mathrm{P} \iff rs \in \mathrm{P}$ e $r \notin$ P, cioè – se P è primo – $s \in$ P e quindi s+P = P: dunque R/P è un dominio di integrità
- $rs \in$ P e $r \notin$ P $\iff (r+\mathrm{P})(s+\mathrm{P})=\mathrm{P}$ e $(r+\mathrm{P}) \neq \mathrm{P}$, cioè – se R/P è un dominio di integrità – s+P = P e quindi $s \in$ P cioè P è primo.

Ne consegue che, visto che ogni campo è un dominio di integrità

OSSERVAZIONE 5.6 *Ogni ideale massimale è primo.*

Il viceversa non è sempre vero [10], anche se vedremo (nel Capitolo II prop. 2.3) che lo è in quei domini di integrità in cui ogni ideale è principale.

[10] Ad esempio, nell'anello di polinomi **Z**[x] l'ideale (x) è primo poiché l'anello quoziente **Z**[x]/(x) è un dominio di integrità essendo isomorfo a **Z**, ma non è massimale poiché l'ideale generato da {2, x} lo contiene propriamente e non esaurisce **Z**[x], non contenendo l'unità.

6. ANELLI DI POLINOMI A COEFFICIENTI IN UN ANELLO

Finora abbiamo usato come esempi di anello **Z** e le classi di resto (oltre ai soliti campi **Q**, **R**, **C**). Un ricchissimo materiale d'esempio (oltre che il soggetto dello studio di questo corso) è dato dagli anelli di polinomi a coefficienti in un anello R, in una o più indeterminate.

Che cosa sono i polinomi in una indeterminata a coefficienti in R?
Formalmente sono *sequenze definitivamente nulle di elementi di* R: $(a_0, a_1,\ldots, a_n, 0,\ldots,0,\ldots.)$ con n variabile in **N** e a_k variabili in R. La maniera standard di rappresentarli è

$$a(x) = a_0 + a_1x + \ldots + a_n x^n$$

ove x è detta **indeterminata**, $a_0, \ldots, a_n$ sono detti **coefficienti** ed n è detto **grado del polinomio** (sempre che il coefficiente a_n sia $\neq 0$).
Nell'insieme dei polinomi si introducono le ordinarie operazioni di somma e prodotto, che tengono conto che si vuole che le proprietà della somma e del prodotto definite in R continuino a valere quando si vedono i polinomi come funzioni da R a R e x come variabile invece che come indeterminata (sostanzialmente: segnaposto).
Formalmente, se $a(x) = a_0 + a_1x + \ldots + a_nx^n$ e $b(x) = b_0 + b_1x + \ldots + b_mx^m$,

$$a(x) + b(x) = (a_0+b_0) + (a_1+ b_1)x + \ldots + (a_k+ b_k)x^k,$$

ove k è il massimo tra m e n e, se ad esempio $n>m$, si considerano nulli i coefficienti $b_{m+1},\ldots,b_k$;

$$a(x)b(x) = c_0 + c_1x + \ldots + c_{n+m}x^{n+m}, \qquad \text{ove } c_k = \sum a_i\, b_{k-i}$$

con la somma estesa a tutti gli elementi i cui indici abbiano somma k [(11)].

OSSERVAZIONE 6.1 *L'insieme* R[x] *dei polinomi in una indeterminata x a coefficienti in* R, *rispetto a queste operazioni costituisce un anello che contiene un sottoanello isomorfo a* R, *costituito dai polinomi di grado 0* [(12)].

I polinomi in più indeterminate sono definiti a partire da quelli in una, per ricorrenza.
Si considerano l'anello (R[x])[y] dei polinomi a coefficienti in R[x] in una indeterminata y e l'anello (R[y])[x] dei polinomi a coefficienti in R[y] in una indeterminata x e se ne prova l'isomorfismo [(13)].
Si denota tale anello con R[x,y] e si dice che è l'anello di polinomi a coefficienti in R in due indeterminate x, y.
Similmente partendo da R[x,y] si definisce l'anello di polinomi a coefficienti in R in tre indeterminate x, y, z e così via.

Quindi in sostanza una parte dei discorsi sui polinomi in più indeterminate può ricondursi a quelli in una indeterminata sola.
Ad esempio, quando succede che un anello di polinomi in una o più variabili è un dominio di integrità? È chiaro che innanzi tutto è necessario che l'anello R sia un dominio, altrimenti ci sono dei polinomi di grado 0 (cioè elementi di R) che hanno prodotto nullo pur essendo diversi dal polinomio nullo. Inoltre vale la seguente

---

11) Attenzione: anche se formalmente nel prodotto compare il termine di grado $n+m$, se R non è un dominio di integrità può succedere che $c_{n+m} = a_nb_m$ sia nullo e quindi del grado del prodotto si può solo dire che è $\leq n+m$.

12) Si lascia al lettore la verifica che valgono le proprietà degli anelli: osserviamo solo che

- l'elemento neutro rispetto alla somma è il polinomio nullo (0,0,0,….): sarà denotato con 0
- $-a(x) = a_0 - a_1x - \ldots - a_nx^n$
- l'elemento neutro rispetto al prodotto è il polinomio (1,0,0,….): sarà denotato con 1.

13) L'applicazione φ è quella che riorganizza i coefficienti in modo da mettere in evidenza nel polinomio in y a coefficienti in R[x] il polinomio in x a coefficienti in R[y]. Ad esempio

$$\varphi(1+2x + (x-x^2)y + (2-3x+x^2)y^3) = 1 + 2y^3 + (2+y-3y^3)x + (-y+y^3)\,x^2.$$

OSSERVAZIONE 6.2 *Sia* R *un dominio di integrità. Allora*

i) R[x] *è un dominio di integrità*

ii) *gli elementi invertibili di* R[x] *sono tutti e soli quelli di* R.

Infatti, se $a(x) = a_0 + a_1x + \dots + a_nx^n$ è un polinomio non nullo di grado n e $b(x) = b_0 + b_1x + \dots + b_mx^m$ un altro polinomio, perché sia $a(x)b(x) = 0$ si deve avere

$$c_{n+m} = a_nb_m = 0 \text{ cioè } b_m = 0 \text{ poiché R è un dominio.}$$

Questo significa che in realtà $b(x)$ ha grado inferiore a m: iterando il ragionamento si vede alla fine che $c_{n+0} = a_nb_0 = 0$ cioè $b(x) = b_0 = 0$. Dunque R[x] è un dominio di integrità.

Ora in un dominio di integrità il grado di $a(x)b(x)$ è la somma dei gradi di $a(x)$ e di $b(x)$: quindi se $a(x)b(x) = 1$ la somma dei gradi di $a(x)$ e di $b(x)$ deve essere zero, cioè entrambi i polinomi sono in realtà elementi di R, invertibili in R poiché si deve avere $a_0b_0 = 1$.

Di qui, per induzione [14] si prova il

COROLLARIO 6.3 *Se* R *è un dominio di integrità, è un dominio di integrità anche l'anello di polinomi in* $n \geq 1$ *indeterminate* R[$x_1, \dots, x_n$].

ESEMPI 6.4

a) Se R è un campo k, $k[x]$ è un dominio di integrità e sono invertibili tutti e soli i polinomi "costanti" non nulli: $a(x) = a_0$.
b) Se R = **Z**, **Z**[x] è un dominio di integrità e sono invertibili solo i polinomi 1 e –1.
c) Se R = $k[x_1, \dots, x_n]$, R[x] $k[x_1, \dots, x_n, x]$ è un dominio di integrità e sono invertibili tutti i polinomi che appartengono a $k \setminus \{0\}$.
d) Se R non è un dominio di integrità l'osservazione 6.2 è falsa. Ad esempio in $\mathbf{Z}_4[x]$ si ha $(2x)^2 = 0$ e $(1+2x)^2 = 1$ (ove per brevità con 2 si è indicata la classe di resto mod4 che ha 2 per rappresentante).

Prima di passare a riassumere alcuni fatti noti sui polinomi in una sola indeterminata, diamo un po' di terminologia valida qualunque sia il numero delle indeterminate.

DEFINIZIONE 6.5 *Diremo*

- ***Monomio*** [15] *un polinomio di* R[$x_1, \dots, x_n$] *della forma* $x_1^{\alpha_1} \dots x_n^{\alpha_n} := \boldsymbol{x}^{\boldsymbol{\alpha}}$ ove $(\alpha_1, \dots, \alpha_n) \in \mathbf{N}^n$ (ove **N** denota come sempre l'insieme dei numeri naturali compreso 0).
- ***Multigrado*** *(o logaritmo)* ***del monomio*** *la n-upla* $\boldsymbol{\alpha} = (\alpha_1, \dots, \alpha_n)$ *degli esponenti delle indeterminate del monomio, ordinata secondo l'ordinamento dato alle indeterminate.*
- ***Grado totale del monomio*** [16] *la somma di tali esponenti:* $|\boldsymbol{\alpha}| = \alpha_1 + \dots + \alpha_n$.
- ***Supporto di un polinomio*** *di* R[$x_1, \dots, x_n$] *l'insieme dei monomi che compaiono in esso con coefficiente non nullo.*
- ***Grado del polinomio*** *il massimo tra i gradi totali dei monomi del supporto* [17].

Notiamo che l'insieme dei monomi di R[$x_1, \dots, x_n$], rispetto al prodotto, costituisce un monoide isomorfo al monoide additivo $\mathbf{N}^n$; l'isomorfismo è dato proprio dalla corrispondenza

$$x_1^{\alpha_1} \dots x_n^{\alpha_n} \to (\alpha_1, \dots, \alpha_n).$$

---

[14] Il primo passo è stato provato nell'osservazione 6.2; l'ipotesi induttiva è che sia un dominio di integrità l'anello R[$x_1, \dots, x_{n-1}$] e ancora l'oss.6.2 ove R:= R[$x_1, \dots, x_{n-1}$] dimostra la validità del passo induttivo.

[15] Nei testi di Robbiano, e in particolare in CoCoa, questi oggetti sono chiamati termini mentre sono chiamati monomi quelli che noi chiameremo **termini**, cioè i monomi moltiplicati per coefficiente che compaiono come addendi nel polinomio.

[16] Nei testi di Robbiano deg($\mathbf{x}^{\boldsymbol{\alpha}}$).

[17] Notare che se $n>1$ ci può essere più di un monomio di grado massimo in un polinomio: ad esempio $x+y$ presenta due monomi di primo grado.

7. POLINOMI IN UNA INDETERMINATA

Ogni polinomio di R[x] ha un solo monomio di grado massimo. Allora se il polinomio ha la forma

$$f = a_0 + a_1x + \ldots + a_nx^n$$

con $a_n \neq 0$, diremo che a_nx^n è il **termine direttore** (leading term) del polinomio e lo denoteremo con LT(f) [18]. Diremo inoltre che a_n è il **coefficiente direttore** (leading coefficient) del polinomio e lo denoteremo con Lc(f). Vale il seguente

TEOREMA 7.1 (algoritmo della divisione) *Sia* $d \in$ R[x] *un polinomio con coefficiente direttore invertibile in* R. *Ogni polinomio* $f \in$ R[x] *si può scrivere in maniera unica come*

$$f = dq + r, \quad con\ q, r \in \mathrm{R}[x]$$

ed r=0 *oppure* grado(r)<grado(d).
Inoltre c'è un algoritmo per calcolare il quoziente q *e il resto* r.

Ci limitiamo a proporre l'algoritmo, senza mostrare né che termina (cosa abbastanza facile a verificare basandosi sul fatto che il grado è un numero naturale e che i naturali sono ben ordinati), né che produce esattamente quoziente e resto (cosa ovvia per costruzione, se si accetta che quoziente e resto sono unici: si provi a verificare quest'ultimo fatto).

Input: d, f
Output: q, r
q: = 0; r: = f
WHILE $r \neq 0$ AND LT(d) divide LT(r) DO
q: = q + (LT(r)/LT(d))
r: = r – (LT(r)/LT(d)) d

Ad esempio, se $f = 4x^3+2x^2-x+1$ e $d = 2x+1$ sono polinomi in **Q**[x] si ha LT(d) = $2x$. Allora

	Partenza	Passo 1	Passo 2	STOP
q	0	$0+4x^3/2x=2x^2$	$2x^2+(-x)/2x=2x^2-1/2$	**Quoziente**
r	$4x^3+2x^2-x+1$	$4x^3+2x^2-x+1-2x^2(2x+1)= -x+1$	$-x+1-(-1/2)(2x+1)=3/2$	**resto**
LT(r)	$4x^3$	$-x$	3/2	
LT(d) divide LT(r)?	SÌ	SÌ	NO	

A parte la diversa raffigurazione grafica è esattamente quel che si è imparato a fare per dividere due polinomi:

$$\begin{array}{l|l} 4x^3+2x^2-x+1 & 2x+1 \\ \hline -2x^2(2x+1) & 2x^2-1/2 \\ \hline \quad -x+1 & \\ -(-1/2)(2x+1) & \\ \hline \quad 3/2 & \end{array}$$

NOTA 7.2 Il teorema non richiede che R sia un campo e neppure un dominio di integrità: chiede solo che il coefficiente direttore del divisore sia invertibile. Nel caso in cui R sia un campo ciò equivale a chiedere che il polinomio divisore sia diverso da zero, negli altri casi la richiesta è più forte. In ogni caso, notiamo che, se il coefficiente direttore del divisore è 1 le cose vanno bene.
Ciò rende vero in ogni anello di polinomi R[x] il cosiddetto

[18] Vedremo come nel caso dei polinomi di più variabili la scelta di quale termine considerare direttore non sia così ovvia e sia determinante per gli sviluppi successivi.

TEOREMA DI RUFFINI *Ogni polinomio f nella divisione per $(x - c)$ ha resto $f(c)$ e quindi f è divisibile per $(x - c)$ se e solo se $f(c) = 0$* [19].

COROLLARIO 7.3 *Se il polinomio f non è nullo e ha grado m, allora ha al più m radici in* R.

Infatti se $m = 0$, f è una costante non nulla e quindi il polinomio ha 0 radici.
Se $m > 0$, o f non ha radici (e allora il numero di radici è $<m$) oppure, se c è una radice, risulta $f = (x - c)q$ e il grado di q è $m - 1$: per induzione si ha la tesi.

Ne consegue un enunciato valido per polinomi in un numero qualunque di indeterminate:

TEOREMA 7.4 *Sia* R *infinito*[20]. *$f \in R[x_1,\ldots,x_n]$ è il polinomio nullo se e solo se la corrispondente funzione f: $R^n \to R$ è la funzione identicamente nulla.*

Dimostrazione È ovvio che il polinomio nullo dà luogo alla funzione nulla.
Viceversa, procediamo per induzione sul numero di indeterminate.
Se $n = 1$, un polinomio non nullo ha un numero di radici al più pari al suo grado ed, essendo infiniti gli elementi di R, non può annullarsi in tutti.
Se $n>1$ e $f(c_1,\ldots,c_n) = 0$ per tutte le n-uple $(c_1,\ldots,c_n)$ di R^n, riscriviamo f come polinomio di $(R[x_1,\ldots, x_{n-1}])[x_n]$:

$$f = a_0(x_1,\ldots,x_{n-1}) + a_1(x_1,\ldots,x_{n-1})x_n + \ldots + a_m(x_1,\ldots,x_{n-1})x_n^m.$$

Per ogni $(c_1,\ldots,c_{n-1}) \in R^{n-1}$, il polinomio di $R[x_n]$:

$$h(x_n) = a_0(c_1,\ldots,c_{n-1}) + a_1(c_1,\ldots,c_{n-1})x_n + \ldots + a_m(c_1,\ldots,c_{n-1})x_n^m$$

si annulla su tutto R e quindi è il polinomio nullo, cioè tutti i coefficienti $a_i(c_1,\ldots,c_{n-1})$ sono nulli, per ogni $(c_1,\ldots,c_{n-1})$ di R^{n-1}. Per l'ipotesi induttiva ciò significa che ogni $a_i(x_1,\ldots,x_{n-1})$ è il polinomio nullo e quindi anche f lo è. C.V.D

Supponiamo infine che l'anello R sia un campo k. Dal teorema 7.1 si deduce la seguente

OSSERVAZIONE 7.5 *Ogni ideale dell'anello $k[x]$ dei polinomi a coefficienti in un campo è principale. Inoltre, a meno di prodotti per elementi non nulli del campo, il generatore dell'ideale è unico.*
Non diamo la dimostrazione di questa proprietà che dimostreremo in generale per i cosiddetti domini euclidei (Capitolo II, osservazione 3.4)

È invece interessante capire come trovare il generatore di un ideale di $k[x]$ assegnato dando un numero finito di generatori, ad esempio $I=(x^4-1, x^6-1)$.

OSSERVAZIONE 7.6 *Dati due polinomi f, g non nulli in $k[x]$*
i) esiste il massimo comun divisore di f e g ed è unico a meno della moltiplicazione per un elemento non nullo del campo
ii) esso genera l'ideale (f, g)
iii) c'è un algoritmo per calcolarlo.

---

[19] Come è ben noto, ad ogni polinomio $f = a_0 + a_1x + \ldots + a_nx^n \in R[x]$ è associata la funzione f: $R \to R$ che ad ogni $c \in R$ associa la valutazione $f(c) = a_0 + a_1c + \ldots + a_nc^n$ del polinomio in c.
In particolare se $f(c) = 0$ si usa dire che c è una **radice** del polinomio f. La dimostrazione del teorema è un'applicazione dell'algoritmo della divisione: infatti $f = (x - c)q + r$ con grado$(r)<1$ cioè $r \in R$. Ponendo $x = c$ si ha la tesi.

[20] Se l'anello R è finito il teorema non è più vero: infatti, se $R = \{c_1, c_2, \ldots, c_m\}$, il polinomio $f(x) = (x - c_1)\cdot\ldots\cdot(x - c_m)$ si annulla in tutti gli elementi di R pur non essendo il polinomio nullo.

La dimostrazione dei primi due punti verrà fatta in generale nella proposizione 3.6 del Capitolo II ed è quindi inutile proporla qui. Vediamo invece l'algoritmo.

Input: f, g
Output: h [= MCD(f, g)]
$h := f$; $s := g$
WHILE $s \neq 0$ DO
    $r :=$ resto(h, s) [output dell'algoritmo della divisione di h per s]
    $h := s$
    $s := r$

L'algoritmo termina poiché a ogni passo il grado di s si abbassa (e **N** è ben ordinato). Inoltre a ogni passo MCD(h, s)=MCD(s, r), poiché se

$$h = sq + r,$$

ogni d che divida tanto s che r divide anche h e viceversa ogni d che divida tanto h che s divide anche r.
Se, al passo in cui l'algoritmo termina, il divisore è $\bar{s}$, si ha MCD(f, g) = $\bar{s}$.
I quozienti che si incontrano passo a passo servono a individuare i polinomi a, b tali che $af + bg = \bar{s}$.

ESEMPI 7.7
a) Se $f = x^6 - 1$ e $g = x^4 - 1$, si ha $x^6 - 1 = x^2(x^4 - 1) + x^2 - 1$; $x^4 - 1 = (x^2 + 1)(x^2 - 1)$ $\Rightarrow$ $x^2 - 1 = (x^6 - 1) - x^2(x^4 - 1)$.
b) Se $f = x^4 + 3x^3 + x^2 - 3x - 2$ e $g = x^4 - x^3 - 11x^2 + 9x + 18$, si ha

	Passo 0	Passo 1	Passo 2	Passo 3
h	$x^4+3x^3+x^2-3x-2$	$x^4-x^3-11x^2+9x+18$	$4x^3+12x^2-12x-20$	$4x^2+2x-2$
s	$x^4-x^3-11x^2+9x+18$	$4x^3+12x^2-12x-20$	$4x^2+2x-2$	$-15x-15$
r	$4x^3+12x^2-12x-20$	$4x^2+2x-2$	**$-15x-15$**	**0**
q	1	$x/4-1$	$x+5/2$	$-4/15x+2/15$
$r=ah+bs$	$f-1g$	$g-(f-g)\cdot(x/4-1)$	**$f-g-[f\cdot(1-x/4)+g\cdot x/4](x+5/2)$**	

e quindi $-15x-15 = f\cdot(x^2/4-3x/8-3/2) - g\cdot(x^2/4+5x/8+1)$ o, se si preferisce
$x+1 = g\cdot(x^2/60+x/24+1/15) - f\cdot(x^2/60-3x/120-1/10)$.

Iterando il procedimento si trova il MCD di più di due polinomi.

Concludendo:
In $k[x]$ se un ideale è assegnato tramite i suoi generatori, applicando ripetutamente l'algoritmo euclideo per il calcolo del MCD si trova una base per l'ideale formata da un sol elemento.
Questa base è particolarmente significativa poiché *fornisce uno strumento per stabilire se un polinomio appartiene all'ideale oppure no* (basta vedere se il generatore divide il polinomio).

Il progetto che svilupperemo nei capitoli successivi al secondo è di *trovare uno strumento analogo anche in anelli di polinomi su un campo in più indeterminate*.
I problemi che si incontrano sono legati al fatto che
- in tali anelli non tutti gli ideali sono principali
- negli analoghi dell'algoritmo della divisione che si riescono ad inventare (che dipendono dall'ordinamento scelto sui monomi) l'unicità del resto dipende pesantemente dal sistema di divisori.

8. CAMPI ALGEBRICAMENTE CHIUSI

DEFINIZIONE 8.1 *Un campo k è detto* ***algebricamente chiuso*** *se ogni polinomio f del dominio $k[x]$ di grado $m \geq 1$ ha almeno una radice in k, cioè esiste un $c_1 \in k$ tale che $f(c_1)=0$.*

In un campo algebricamente chiuso il corollario 7.3 si precisa come segue:

PROPOSIZIONE 8.2 *Se il campo k è algebricamente chiuso ogni polinomio $f \in k[x]$ di grado $m \geq 1$ si può scrivere come prodotto di esattamente m polinomi di primo grado di $k[x]$ (eventualmente coincidenti, del tutto o in parte):*

(*) $$f(x) = a\,(x - c_1)\,(x - c_2)\cdot\ldots\cdot(x - c_m) \qquad a, c_1, \ldots, c_m \in k$$

e quindi ha <u>esattamente</u> m <u>radici</u> $c_1, \ldots, c_m$ in k, pur di contare la radice di ogni polinomio $(x - c_i)$ che compaia eventualmente più volte in (*) con la molteplicità corrispondente.

Dimostrazione Proviamo l'enunciato per induzione sul grado m del polinomio. L'enunciato è banalmente vero se $m=1$; supposto che sia vero per ogni polinomio di grado $m-1$ mostriamo che vale per ogni polinomio di grado m. Essendo k algebricamente chiuso esiste un $c_1 \in k$ tale che $f(c_1)=0$ e quindi, per il teorema di Ruffini, $f(x)$ è divisibile per $(x - c_1)$ cioè si può scrivere

$$f(x) = (x - c_1)\,f_2(x),$$

ove $f_2(x)$ è un polinomio di grado $m-1$. Per l'ipotesi induttiva esistono m elementi $a, c_2, \ldots c_m$ di k tali che $f_2(x) = a\,(x - c_2)\cdot\ldots\cdot(x - c_m)$ e quindi $f(x) = a\,(x - c_1)\,(x - c_2)\cdot\ldots\cdot(x - c_m)$. C.V.D.

ESEMPI 8.3

a) Il campo $\mathbf{Z}_2$ non è algebricamente chiuso poiché $x^2 + x + 1$ non ha radici in $\mathbf{Z}_2$.
b) Si dimostra invece che è algebricamente chiuso il campo complesso $\mathbf{C}$.
c) Un altro esempio di campo algebricamente chiuso è costituito dal campo dei numeri algebrici, definito come il più piccolo campo algebricamente chiuso contenente il campo $\mathbf{Q}$ dei numeri razionali (cioè, come si usa dire, la chiusura algebrica di $\mathbf{Q}$): esso contiene tutti quei numeri reali o complessi (come ad esempio $\sqrt{2}$, $\sqrt{-1}$, $\sqrt[3]{5}$, $1-\sqrt{-3}$ …) che sono soluzioni di equazioni algebriche a coefficienti in $\mathbf{Q}$, cioè che sono radici di polinomi a coefficienti interi.

In generale, a partire da un qualunque campo, anche finito, è possibile costruire un campo algebricamente chiuso che lo contenga. Ma:

TEOREMA 8.4 *Ogni campo k algebricamente chiuso è infinito.*

Dimostrazione [21] Proviamo la contronominale: sia k un campo finito e siano $\{c_1, \ldots, c_{m-1}, c_m = 0\}$ i suoi elementi, a due a due distinti. Il polinomio $p(x) = x\,(x - c_1)\cdot\ldots\cdot(x - c_{m-1}) + 1$ ha grado $m \geq 1$ ma non è divisibile per alcuno dei polinomi di primo grado di $k[x]$ visto che il resto nella divisione per ognuno di essi è 1. Quindi $p(x)$ non può essere scritto come prodotto di m polinomi di primo grado di $k[x]$ e di conseguenza il campo k non è algebricamente chiuso. C.V.D.

[21] Sono possibili varie dimostrazioni: una fa appello al teorema di Fermat (che afferma che in ogni campo finito con m elementi ogni elemento soddisfa l'equazione $x^m = x$); di un'altra si fornisce uno schizzo negli esercizi. Quella presentata qui è una rivisitazione dell'argomento di Euclide per dimostrare l'esistenza di infiniti numeri primi: visto che nel dominio $k[x]$ sono i polinomi irriducibili che assumono il ruolo giuocato dai numeri primi nel dominio degli interi (vedi nel Capitolo II il discorso sulla fattorizzazione) e visto che se k è algebricamente chiuso gli unici polinomi irriducibili sono quelli di primo grado, è ovvio che tale argomento "funzioni".

9. APPENDICE: CLASSI DI RESTO MODULO *n*

Richiamiamo velocemente alcune informazioni sulle classi di resto modulo n.

Innanzi tutto, in $\mathbf{Z}$ vale un algoritmo della divisione (come in $k[x]$), cioè fissati due numeri interi m e n (con $n \neq 0$) esistono (e sono unici) $q, r \in \mathbf{Z}$ tali che $m = nq + r$ con $0 \leq r < n$ (ovviamente q è il quoziente e r il resto nella divisione).

Si possono allora considerare i sottoinsiemi di $\mathbf{Z}$ formati dai numeri m che divisi per n danno lo stesso resto: per quanto appena detto ogni numero intero appartiene a uno ed uno solo di tali sottoinsiemi. Ogni sottoinsieme cosiffatto verrà detto **classe di resto modulo *n*** e sarà denotato con $[m]_n$, se m è un suo elemento; in particolare, se il resto è r, si potrà indicare con $[r]_n$. L'insieme delle classi di resto modulo n è denotato con $\mathbf{Z}_n$.
In questo insieme si introducono una somma e un prodotto definendo

$$[m]_n + [m']_n = [m+m']_n \qquad \text{e} \qquad [m]_n \cdot [m']_n = [m \cdot m']_n$$

Si verifica che tali operazioni non dipendono dai rappresentanti scelti (sostanzialmente si passa al quoziente - vedi definizione 4.4 - di $\mathbf{Z}$ rispetto ad $n\mathbf{Z}$ e quindi la verifica è analoga).
Rispetto a queste operazioni $\mathbf{Z}_n$ è un anello con zero $[0]_n = [n]_n$ ed unità $[1]_n$.

Ci si può chiedere quando tale anello ha divisori dello zero.
Ciò equivale a chiedere per quali n esistono interi m, m' non divisibili per n, tali che $m \cdot m' = kn$ (con k intero). Ciò non può mai succedere se n è un numero primo (in tal caso, per il teorema di fattorizzazione unica in primi, uno dei fattori di m e/o m' dovrebbe essere n), mentre è sicuramente possibile se n è il prodotto di due o più primi (eventualmente coincidenti): infatti se $n = r \cdot s$ si ha $[0]_n = [n]_n = [r \cdot s]_n = [r]_n \cdot [s]_n$ e sicuramente n non divide r né s.
Quindi $\mathbf{Z}_n$

- se n primo, è un dominio di integrità (finito e quindi è un campo)
- se n non è primo, ha divisori dello zero (le classi rappresentate dai prodotti di una parte dei fattori di n)
- se n ha tra i suoi fattori almeno una potenza di un numero primo con esponente >1, ha anche elementi nilpotenti, cioè tali che una loro potenza è 0.

Ad esempio in $\mathbf{Z}_4$: $[2]_4^2=[0]_4$; in $\mathbf{Z}_{72}$: $[6]_{72}^3=[2^3 \cdot 3^2 \cdot 3]_{72}=[72]_{72} \cdot [3]_{72}=[0]_{72}$ e analogamente per tutte le classi aventi rappresentanti multipli di 6 minori di 72.

Quali sono gli ideali di $\mathbf{Z}_n$?
Sappiamo (vedi conseguenze del 1° teorema di isomorfismo) che l'immagine inversa $\varphi^{-1}(I)$ di un ideale I di $\mathbf{Z}_n$ mediante l'omomorfismo canonico $\varphi: \mathbf{Z} \to \mathbf{Z}_n$ è un ideale di $\mathbf{Z}$ che contiene $\ker(\varphi)=n\mathbf{Z}$. Innanzi tutto bisogna quindi scoprire quali sono gli ideali di $\mathbf{Z}$: poiché vale l'algoritmo della divisione, tutti gli ideali di $\mathbf{Z}$ sono principali (vedi Capitolo II osservazione 3.4). $n\mathbf{Z}$ è contenuto in un ideale $m\mathbf{Z}$ se e solo se m divide n e quindi gli ideali di $\mathbf{Z}_n$ sono gli insiemi di elementi della forma

$$m\mathbf{Z}_n = \{[mz]_n \text{ con } m \text{ divisore fissato di } n \text{ e } z \in \mathbf{Z}\}.$$

Inoltre l'ideale $m\mathbf{Z}_n$ contiene l'ideale $m'\mathbf{Z}_n$ se e solo se m divide m'.

10. ESERCIZI

1) Dimostrare che se in un insieme S si introduce un'operazione binaria $*$ associativa ed
   - esiste un elemento e di S tale che per ogni $s \in$ S risulti: $s*e = s$
   - per ogni $s \in$ S esiste un elemento s' (chiamiamolo inverso destro di s) tale che: $s*s' = e$

   allora si ha anche $s'*s = e$ (ove s' è l'inverso destro di s) ed $e*s = s$, cioè (S,$*$) è un gruppo.
   Provare inoltre che l'elemento neutro in un monoide e l'inverso di un elemento in un gruppo sono unici. (Risposta)

2) Quali sono gli ideali di $\mathbf{Z}_{30}$? Quali catene di inclusioni tra questi ideali posso formare? Come posso tener conto contemporaneamente di tutte queste catene? $18\mathbf{Z}_{30}$ rappresenta un ideale di $\mathbf{Z}_{30}$? Se sì, quale? In generale, se $m<n$ non divide n, come posso stabilire chi è l'ideale $m\mathbf{Z}_n$? $34\mathbf{Z}_{30}$ rappresenta un ideale di $\mathbf{Z}_{30}$? Se sì, quale? In generale, se m è maggiore di n, come posso stabilire chi è l'ideale $m\mathbf{Z}_n$? (Risposta)

3) Consideriamo l'anello $R=\mathbf{Z}_2[x]$ dei polinomi a coefficienti in $\mathbf{Z}_2$ in una indeterminata. Denotate le classi di resto [0] e [1] rispettivamente con 0 e 1, il polinomio x^2+x+1 si può scrivere come prodotto di polinomi di primo grado a coefficienti in $\mathbf{Z}_2$?
   Sia I l'ideale generato in R dal polinomio x^2+x+1. Quanti elementi ha l'anello quoziente R/I? Che tipo di anello è? Contiene un sottocampo isomorfo a $\mathbf{Z}_2$? (Risposta)

4) Consideriamo il dominio S_p introdotto negli esercizi 2.2 d. Verificare che pS_p è un ideale massimale, anzi l'unico ideale massimale di S_p. A chi è isomorfo l'anello quoziente S_p/pS_p? (Risposta)

5) Siano $\{c_1,\ldots, c_{m-1}, c_m\}$ m elementi distinti di un campo k. Mostrare che
   a) è possibile trovare un polinomio di grado $\leq m-1$ a coefficienti in k la cui corrispondente funzione assume in $c_1,\ldots, c_m$ rispettivamente i valori $d_1, \ldots, d_m$ non necessariamente distinti;
   b) tale polinomio ha grado $r \geq 1$ se e solo se almeno due elementi d_i e d_j $(i \neq j)$ sono distinti.
   c) Utilizzare questa osservazione per una dimostrazione alternativa del fatto che se k è un campo finito non può essere algebricamente chiuso. (Risposta)

Soluzioni.

1)
Siano s' ed s'' gli inversi destri rispettivamente di s ed s': $s*s' = e = s'*s''$.
Proviamo innanzi tutto che $s'*s = e$, cioè s' è l'inverso anche sinistro di s. Tale prodotto è un elemento x di S ed, essendo e unità destra e $*$ associativa,

$$s'*s = x = x*e = (s'*s) * (s'*s'') = s' * (s*s') * s'' = (s'*e) * s'' = s'*s'' = e.$$

Ora vediamo che e è anche neutro a sinistra:

$$e*s = (s*s') * s = s * (s'*s) = s * e = s.$$

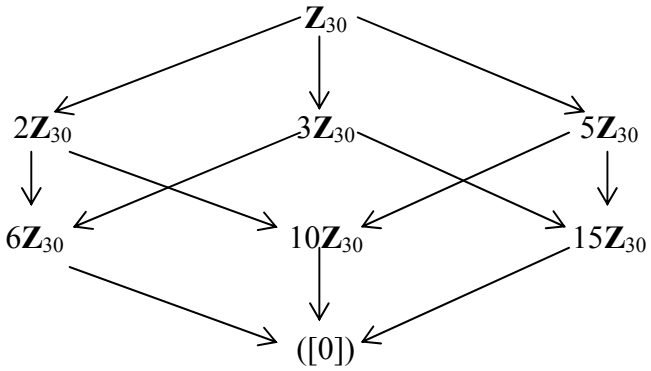
Sia ora (S,$*$) un monoide. Se e ed e' sono entrambi elementi neutri in (S,$*$) si deve avere $e = e*e' = e'$.
Sia infine (S,$*$) un gruppo ed e il suo elemento neutro: se s' ed s'' sono due inversi di $s \in$ S risulta

$$s' = e*s' = (s''*s) * s' = s''* (s*s') = s''*e = s''.$$

2)
Gli ideali non banali di $\mathbf{Z}_{30}$ sono
$2\mathbf{Z}_{30}$={[0],[2],[4],[6],[8],[10],[12],[14],[16],[18],[20],[22],[24],[26],[28]}
$3\mathbf{Z}_{30}$={[0],[3],[6],[9],[12],[15],[18],[21],[24],[27]}
$5\mathbf{Z}_{30}$={[0],[5],[10],[15],[20],[25]}
$6\mathbf{Z}_{30}$={[0],[6],[12],[18],[24]}
$10\mathbf{Z}_{30}$={[0],[10],[20]}
$15\mathbf{Z}_{30}$={[0],[15]}

Valgono le seguenti catene di inclusione
$([0])\subset 6\mathbf{Z}_{30}\subset 2\mathbf{Z}_{30}\subset \mathbf{Z}_{30}$
$([0])\subset 6\mathbf{Z}_{30}\subset 3\mathbf{Z}_{30}\subset \mathbf{Z}_{30}$
$([0])\subset 10\mathbf{Z}_{30}\subset 2\mathbf{Z}_{30}\subset \mathbf{Z}_{30}$
$([0])\subset 10\mathbf{Z}_{30}\subset 5\mathbf{Z}_{30}\subset \mathbf{Z}_{30}$
$([0])\subset 15\mathbf{Z}_{30}\subset 3\mathbf{Z}_{30}\subset \mathbf{Z}_{30}$
$([0])\subset 15\mathbf{Z}_{30}\subset 5\mathbf{Z}_{30}\subset \mathbf{Z}_{30}$

che si possono raccogliere nel seguente reticolo



ove la freccia A $\rightarrow$ B deve essere intesa come A $\supset$ B.

L'insieme $18\mathbf{Z}_{30}$ è ancora un ideale di $\mathbf{Z}_{30}$ (si potrebbero verificare le proprietà di chiusura) e quindi deve coincidere con uno di quelli precedentemente listati. Poiché $18=2\cdot 3\cdot 3$, la classe [18] appartiene solo a $2\mathbf{Z}_{30}$, $3\mathbf{Z}_{30}$, $6\mathbf{Z}_{30}$ e quindi $18\mathbf{Z}_{30}$ è contenuto in questi ideali e in particolare coincide con il più piccolo dei tre $6\mathbf{Z}_{30}= 2\mathbf{Z}_{30}\cap 3\mathbf{Z}_{30}$.
Quindi, in generale, se $m<n$, ma m non divide n, bisogna trovare il massimo comun divisore d tra n ed m: l'ideale $d\mathbf{Z}_n$ conterrà $[m]$ e sarà il più piccolo ideale con questa proprietà e quindi $d\mathbf{Z}_n = m\mathbf{Z}_n$.

L'insieme $34\mathbf{Z}_{30}$ è ancora un ideale di $\mathbf{Z}_{30}$ e quindi deve coincidere con uno dei precedenti. Poiché $34>30$, e $34=30\cdot 1+4$ risulterà $34\mathbf{Z}_{30} = 4\mathbf{Z}_{30} = 2\mathbf{Z}_{30}$.
In generale, se r è il resto nella divisione di m per n, si ha $r\mathbf{Z}_n = m\mathbf{Z}_n$; utilizzando poi la strategia vista sopra, se r non divide n si riconduce l'ideale $r\mathbf{Z}_n$ all'ideale $d\mathbf{Z}_n$, con d=MCD(r,n).

3)
Se si potesse scrivere il polinomio $f=x^2+x+1$ come prodotto di due polinomi di primo grado, ci sarebbe un polinomio di primo grado $x-a$ che divide f e quindi ci sarebbe un elemento $a\in\mathbf{Z}_2$ tale che $f(a)=0$. Ma $f(0)=1$ e $f(1)=1+1+1=1$. Quindi f non si può scrivere come prodotto di due polinomi di primo grado a coefficienti in $\mathbf{Z}_2$.
Quando si fa il quoziente del dominio $\mathbf{Z}_2[x]$ rispetto all'ideale I generato da f si trovano i laterali I, 1+I, x+I, (x+1)+I, tutti distinti poiché la differenza tra i rappresentanti non può appartenere a I avendo grado <2. D'altra parte ogni polinomio di grado ≥2 diviso per f dà resto 0 o 1 o x o x+1 e quindi cade in una di queste classi laterali: ad esempio $x^2=(x^2+x+1)+x+1$ (in $\mathbf{Z}_2$: $+1=-1$).
Anzi, una maniera semplice per vedere in che laterale cade un polinomio è di sostituire ogni occorrenza di x^2 con x+1.
Ad esempio sostituendo in $x^3+x+1 = x(x^2)+x+1$ si avrà $x(x+1)+x+1 = x^2+1$ e, sostituendo ancora, $x+1+1=x$: quindi x^3+x+1 appartiene a [x]. Nel quoziente diremo addirittura (trascurando le parentesi che denotano i laterali) che $x^2 = x+1$ e che $x^3+x+1 = x$. Concludendo, in R/I ci sono 4 elementi. Dimenticando le parentesi quadre avremo le seguenti tavole di addizione e moltiplicazione:

+	0	1	x	1+x
0	0	1	x	1+x
1	1	0	1+x	x
x	x	1+x	0	1
1+x	1+x	x	1	0

×	0	1	x	1+x
0	0	0	0	0
1	0	1	x	1+x
x	0	x	1+x	1
1+x	0	1+x	1	x

Dalla tabella moltiplicativa si vede che ogni elemento non nullo ha inverso (evidenziato in giallo): quindi R/I è un campo. Le sottotabelle evidenziate in azzurro mettono in evidenza che R/I contiene un sottocampo isomorfo a $\mathbf{Z}_2$ (cioè con le stesse tavole di addizione e moltiplicazione).
Attenzione però: concretamente quel che si denota con 0 e 1

- in $\mathbf{Z}_2$ sono i due laterali $[0]_2$ e $[1]_2$ di $\mathbf{Z}$ formati rispettivamente dai numeri pari e dispari.
- in $\mathbf{Z}_2[x]/I=\mathbf{Z}_2[x]/([1]_2x^2+[1]_2x+[1]_2)$ sono i due laterali I e $[1]_2$+I di $\mathbf{Z}_2[x]$.

4)
L'ideale $p\mathrm{S}_p$ è formato dalle frazioni che, ridotte ai minimi termini, hanno denominatore non divisibile per p e numeratore divisibile per p. È quindi chiaro che ogni frazione r/q che non sta in $p\mathrm{S}_p$ è invertibile e quindi l'ideale $p\mathrm{S}_p+(r/q)\mathrm{S}_p$ coincide con S_p: ciò garantisce che l'ideale è massimale.
Non ci sono ideali non contenuti $p\mathrm{S}_p$ in poiché una frazione per appartenere ad un ideale proprio non deve avere inverso e questo significa che il suo numeratore è multiplo di p cioè sta in $p\mathrm{S}_p$.
Il quoziente $\mathrm{S}_p/p\mathrm{S}_p$ è un campo (per la massimalità dell'ideale) isomorfo a $\mathbf{Z}_p$. Per stabilire l'isomorfismo basta osservare che l'omomorfismo caratteristico φ: $\mathbf{Z}\to\mathrm{S}_p/p\mathrm{S}_p$ definito da $\varphi(z)=z+p\mathrm{S}_p$ ha nucleo $p\mathbf{Z}$ ed è suriettivo. (La suriettività è legata al fatto che, considerando $\mathbf{Z}$ come sottoanello di S_p, risulta $\mathbf{Z}+p\mathrm{S}_p=\mathrm{S}_p$. Poiché p appartiene a $\mathbf{Z}$ si vede che per ogni intero positivo k risulta $\mathbf{Z}+p^k\mathrm{S}_p=\mathrm{S}_p$ e quindi similmente $\mathrm{S}_p/p^k\mathrm{S}_p\cong\mathbf{Z}_{p^k}$).

5)

a) Sia $p(x) = p_0 x^{m-1} + \ldots + p_{m-2}\, x + p_{m-1}$ un polinomio di $k[x]$ con grado $\le m-1$. La condizione $p(c_i)=d_i$ per ogni $i \in \{1, \ldots, m\}$ porta a risolvere un sistema lineare di m equazioni

$$p_0\, c_i^{\,m-1} + \ldots + p_{m-2}\, c_i + p_{m-1} = d_i$$

nelle m incognite $p_0, \ldots, p_{m-1}$ che è risolubile (in maniera unica) poiché la sua matrice dei coefficienti ha determinante (di Vandermond [(22)])

$$[(c_1-c_2)(c_1-c_3)\ldots(c_1-c_m)][(c_2-c_3)\ldots(c_2-c_m)]\cdot\ldots\cdot(c_{m-1}-c_m)$$

sicuramente non nullo poiché i c_i sono tutti distinti.

b) Se $d_i \neq d_j$ il valore del polinomio in questione non è costante e quindi non può essere $p(x) = p_0$, cioè il polinomio ha grado almeno 1.

c) Sia $k = \{c_1, \ldots, c_{m-1}, c_m = 0\}$. Poiché il campo $\mathbf{Z}_2$ non è algebricamente chiuso si può supporre $m \ge 3$. Costruiamo il polinomio $p(x) = p_0 x^{m-1} + \ldots + p_{m-1}$ di grado $r \le m-1$ tale che $p(0)=1$ e $p(c_i)=c_i$ per ogni $i \in \{1, \ldots, m-1\}$; essendo $m \ge 3$, $c_2 \neq 0$ e quindi $p(c_1)=c_1 \neq c_2 = p(c_2)$. Se il campo fosse algebricamente chiuso, il polinomio $p(x)$, avendo grado $r \ge 1$, dovrebbe avere almeno una radice in k, mentre per costruzione il valore di $p(x)$ in ogni c_i è diverso da 0.

[(22)] La matrice dei coefficienti del sistema è $\begin{pmatrix} c_1^{\,m-1} & \cdots & c_1 & 1 \\ c_2^{\,m-1} & \cdots & c_2 & 1 \\ \vdots & & \vdots & \vdots \\ c_m^{\,m-1} & \cdots & c_m & 1 \end{pmatrix}$. Per calcolare il suo determinante, si sottrae la prima riga dalle altre, raccogliendo (per ciascuna riga dalla seconda in poi) il fattore comune agli elementi della riga e poi si sottrae dalla prima la seconda colonna moltiplicata per c_1, dalla seconda la terza moltiplicata c_1 e così via. In tal modo si evidenzia un determinante di Vandermond di ordine m-1 e si itera (con le ovvie sostituzioni). Ad esempio, se $m = 4$,

$$\begin{vmatrix} c_1^3 & c_1^2 & c_1 & 1 \\ c_2^3 & c_2^2 & c_2 & 1 \\ c_3^3 & c_3^2 & c_3 & 1 \\ c_4^3 & c_4^2 & c_4 & 1 \end{vmatrix} = \begin{vmatrix} c_1^3 & c_1^2 & c_1 & 1 \\ c_2^3 - c_1^3 & c_2^2 - c_1^2 & c_2 - c_1 & 0 \\ c_3^3 - c_1^3 & c_3^2 - c_1^2 & c_3 - c_1 & 0 \\ c_4^3 - c_1^3 & c_4^2 - c_1^2 & c_4 - c_1 & 0 \end{vmatrix} = -(c_2-c_1)(c_3-c_1)(c_4-c_1) \begin{vmatrix} c_2^2 + c_2 c_1 + c_1^2 & c_2 + c_1 & 1 \\ c_3^2 + c_3 c_1 + c_1^2 & c_3 + c_1 & 1 \\ c_4^2 + c_4 c_1 + c_1^2 & c_4 + c_1 & 1 \end{vmatrix} =$$

$$= (c_1-c_2)(c_1-c_3)(c_1-c_4) \begin{vmatrix} c_2^2 + c_1(c_2+c_1) & c_2 + c_1(1) & 1 \\ c_3^2 + c_1(c_3+c_1) & c_3 + c_1(1) & 1 \\ c_4^2 + c_1(c_4+c_1) & c_4 + c_1(1) & 1 \end{vmatrix} = (c_1-c_2)(c_1-c_3)(c_1-c_4) \begin{vmatrix} c_2^2 & c_2 & 1 \\ c_3^2 & c_3 & 1 \\ c_4^2 & c_4 & 1 \end{vmatrix} =$$

$$= (c_1-c_2)(c_1-c_3)(c_1-c_4)(c_3-c_2)(c_4-c_2) \begin{vmatrix} c_3+c_2 & 1 \\ c_4+c_2 & 1 \end{vmatrix} = (c_1-c_2)(c_1-c_3)(c_1-c_4)(c_2-c_3)(c_2-c_4)(c_3-c_4)$$