# Appunti di Teoria degli Anelli

**Versione del** 25 Febbraio 2007

Appunti per alcune parti del corso di *Algebra B* tenuto da Roberto Catenacci al Corso di Laurea in Matematica e Applicazioni dell'Università del Piemonte Orientale; tratti, con alcune modifiche e molti tagli dalle *Note per il corso di Algebra* (a.a. 2001/2002) dei prof. R. Schoof (Università di Roma 'Tor Vergata') e L. van Geemen (Università di Milano).

**Testi di riferimento consigliati:**

I.N. Herstein, *Algebra*, Editori Riuniti, 3a edizione, Roma 1994
M. Artin, *Algebra*, Bollati Boringhieri, Torino 1997

## Indice

# 1 Anelli

In questo paragrafo studiamo gli *anelli*. Daremo diversi esempi importanti di anelli ai quali faremo continuamente riferimento in seguito.

**1.1 Definizione.** Un anello *con identità* $R$ è un insieme fornito di due composizioni, *l'addizione* "+" e la *moltiplicazione* "$\cdot$", e di due elementi speciali, lo zero $0 \in R$, e l'identità $1 \in R$, in modo che valgano i seguenti assiomi:

($R_1$) (*Gruppo additivo*) L'insieme $R$ è un gruppo *abeliano* rispetto all'addizione e con elemento neutro 0.

($R_2$) (*Associatività*) Per ogni $x, y, z \in R$

$$(x \cdot y) \cdot z = x \cdot (y \cdot z).$$

($R_3$) (*L'identità*) Per ogni $x \in R$

$$1 \cdot x = x \cdot 1 = x.$$

($R_4$) (*Distributività*) Per ogni $x, y, z \in R$

$$x \cdot (y + z) = x \cdot y + x \cdot z, \qquad (y + z) \cdot x = y \cdot x + z \cdot x.$$

Questi assiomi definiscono precisamente una struttura di anello. In generale su un anello $R$ non valgono necessariamente gli assiomi ($R_5$) e ($R_6$):

($R_5$) (*Commutatività*) Per ogni $x, y \in R$

$$x \cdot y = y \cdot x.$$

($R_6$) (*Inverso moltiplicativo*) Per ogni $x \in R$, $x \neq 0$ esiste $x^* \in R$ tale che

$$x \cdot x^* = x^* \cdot x = 1.$$

Se per un anello $R$ vale ($R_5$), l'anello $R$ si dice *commutativo*. Se vale ($R_6$) e se $R$ non è l'anello banale (si veda l'Esempio 1.3), l'anello $R$ si dice *un anello con divisione*, detto anche *corpo*. Un anello commutativo con divisione si dice un *campo*.

Come al solito, scriveremo spesso $ab$ per il prodotto $a \cdot b$.

**1.2 Esempio.** Con l'addizione e la moltiplicazione introdotte nel primo paragrafo gli insiemi $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ e $\mathbb{H}$ sono anelli. Lasciamo al lettore la facile verifica. Gli anelli $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$ sono

commutativi. Gli anelli $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ e $\mathbb{H}$ sono anelli con divisione. Siccome la moltiplicazione in $\mathbb{H}$ non è commutativa, solo gli anelli $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$ sono campi.

**1.3 Esempio.** (*L'anello banale*) Di solito, in un anello $R$ gli elementi 0 e 1 sono distinti. Se invece $0 = 1$, ogni elemento di $R$ è 0 perché per $x \in R$ vale

$$x = 1 \cdot x = 0 \cdot x = 0.$$

Per l'ultima uguaglianza si veda l'Eserc.(1.C). Dunque, se $0 = 1$, l'anello $R$ è uguale a $\{0\}$. Questo anello si chiama *l'anello banale*.

**1.4 Esempio.** Con l'addizione usuale e la moltiplicazione data da

$$\overline{a} \cdot \overline{b} = \overline{ab},$$

l'insieme $\mathbb{Z}/n\mathbb{Z}$ ha la struttura di anello commutativo. Lasciamo le verifiche al lettore.

**1.5 Esempio.** (*L'anello degli interi di Gauss*) Sia $\mathbb{Z}[i]$ il sottoinsieme di $\mathbb{C}$ dato da

$$\mathbb{Z}[i] = \{a + bi \in \mathbb{C} : \ a, b \in \mathbb{Z}\}.$$

È facile verificare che $\mathbb{Z}[i]$ con l'addizione e la moltiplicazione di $\mathbb{C}$ è un anello commutativo.

**1.6 Definizione.** Sia $R$ un anello. Un elemento $x \in R$ tale che esiste $x^* \in R$ con

$$x \cdot x^* = x^* \cdot x = 1$$

si dice un'*unità* di $R$. L'elemento $x^*$ è l'unico elemento di $R$ che soddisfa $x \cdot x^* = x^* \cdot x = 1$ (si veda l'Eserc. (1.D)) e si dice *l'elemento inverso di* $x$. Si scrive $x^{-1}$ per l'elemento $x^*$. L'insieme delle unità di $R$ si indica con $R^*$.

**1.7 Osservazione.** È da notare che le notazioni $\mathbb{Q}^*$, $\mathbb{R}^*$, $\mathbb{C}^*$ e $\mathbb{H}^*$ coincidono con quelle utilizzate nella parte del corso sui gruppi. Anche la notazione $(\mathbb{Z}/n\mathbb{Z})^*$ coincide: abbiamo già dimostrato che il sottoinsieme $\{\overline{a} : \mathrm{mcd}(a, n) = 1\}$ di $\mathbb{Z}/n\mathbb{Z}$ è un gruppo moltiplicativo. Ogni elemento di questo gruppo ha dunque un inverso moltiplicativo. Viceversa, se $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$ ha un inverso moltiplicativo $\overline{b}$, allora $\overline{a}\,\overline{b} = \overline{1}$, cioè

$$ab = 1 + kn, \qquad \text{per un } k \in \mathbb{Z}.$$

Dunque, ogni divisore comune di $a$ e $n$ divide 1. Concludiamo che $\mathrm{mcd}(a, n) = 1$ e quindi che $\overline{a} \in (\mathbb{Z}/n\mathbb{Z})^*$.

**1.8 Proposizione.** Sia $R$ un anello. Le unità di $R$ formano un gruppo moltiplicativo.

**Dimostrazione.** Ovviamente vale l'assioma dell'associatività. L'identità 1 è l'elemento neutro di $R^*$. Se $a, b \in R^*$ allora

$$(ab)(b^{-1}a^{-1}) = (b^{-1}a^{-1})(ab) = 1$$

e dunque $ab \in R^*$. Finalmente $a^{-1} \in R^*$ se $a \in R^*$. Concludiamo che $R^*$ è un gruppo moltiplicativo. □

**1.9 Esempio.** Per esempio, il gruppo $\mathbb{Z}^*$ è uguale a $\{+1, -1\}$. Si veda l'Eserc.(1.I) per una dimostrazione che $\mathbb{Z}[i]^* = \{\pm 1, \pm i\}$.

**1.10 Proposizione.** Sia $n$ un intero positivo. L'anello $\mathbb{Z}/n\mathbb{Z}$ è un campo se e soltanto se $n$ è un numero primo.

**Dimostrazione.** L'anello $\mathbb{Z}/n\mathbb{Z}$ è un campo se e soltanto se ogni $\overline{x} \in \mathbb{Z}/n\mathbb{Z} - \{0\}$ ha un inverso moltiplicativo. Cioè $\mathbb{Z}/n\mathbb{Z}$ è un campo se e soltanto se

$$(\mathbb{Z}/n\mathbb{Z})^* = \mathbb{Z}/n\mathbb{Z} - \{0\}.$$

Equivalentemente, ogni $a \in \mathbb{Z}$ con $0 < a < n$ ha la proprietà $\mathrm{mcd}(a, n) = 1$. Questo è possibile se e soltanto se $n$ è un numero primo, come richiesto. □

**1.11 Esempio.** Visto che 11 è un primo, l'anello $\mathbb{Z}/11\mathbb{Z}$ è un campo. Gli inversi degli elementi di $\mathbb{Z}/11\mathbb{Z}$ sono:

$$\bar{1}^{-1} = \bar{1}, \quad \bar{2}^{-1} = \bar{6}, \quad \bar{3}^{-1} = \bar{4}, \quad \bar{5}^{-1} = \bar{9}, \quad \bar{7}^{-1} = \bar{8}, \quad \overline{10}^{-1} = \overline{10}.$$

e, ovviamente, $\bar{4}^{-1} = \bar{3}$ etc. La verifica è facile, per esempio $\bar{5} \cdot \bar{9} = \overline{45} = \bar{1}$ quindi $\bar{5}^{-1} = \bar{9}$ e $\bar{9}^{-1} = \bar{5}$.

**1.12 Definizione.** Sia $R$ un anello. Un elemento $a \in R$ si dice un *divisore di zero sinistro* se $a \neq 0$ e se esiste $b \in R$ con $b \neq 0$ e $ab = 0$. L'elemento $a \in R$ si dice un *divisore di zero destro* se $a \neq 0$ e se esiste $b \in R$ con $b \neq 0$ e $ba = 0$. L'elemento $a \in R$ si dice un *divisore di zero* se è un divisore di zero sia destro che sinistro.

**1.13 Esempi.** Negli anelli soliti $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ non ci sono divisori di zero. Ma esistono in altri anelli. Per esempio, in $\mathbb{Z}/6\mathbb{Z}$ si ha $\overline{2} \cdot \overline{3} = \overline{6} = \overline{0}$.

**1.14 Proposizione.** Un'unità di un anello $R$ non può essere un divisore di zero.

**Dimostrazione.** Supponiamo che $a$ sia un'unità ed anche un divisore di zero. Dunque esistono elementi $b, c \in R$ con

$$ab = 1, \qquad ca = 0, \quad (c \neq 0).$$

Abbiamo

$$0 = 0 \cdot b = (ca) \cdot b = c \cdot (ab) = c \cdot 1 = c,$$

contraddicendo $c \neq 0$. □

**1.15** Dunque, gli anelli con divisione non possiedono divisori di zero, perché ogni elemento non nullo è un'unità. Più generalmente, ogni sottoanello (si veda l'Esempio 1.18) di un anello

con divisione non contiene divisori di zero. L'anello $\mathbb{Z}$ e l'anello degli interi di Gauss $\mathbb{Z}[i]$ ne sono esempi.

**1.16 Definizione.** Un anello non banale che è commutativo e non possiede divisori di zero si dice un *dominio di integrità*.

**1.17 Esempi.** I campi sono esempi di domini di integrità. Come abbiamo visto sopra, anche i sottoanelli dei campi sono domini di integrità. Per esempio $\mathbb{Z} \subset \mathbb{R}$ e l'anello degli interi di Gauss $\mathbb{Z}[i] \subset \mathbb{C}$ sono domini di integrità.

Per ottenere altri esempi di anelli, consideriamo adesso diversi metodi per costruire nuovi anelli a partire da anelli dati.

**1.18 Sottoanelli.** Sia $R$ un anello. Un *sottoanello di* $R$ è un sottoinsieme di $R$ il quale è, con la stessa addizione e moltiplicazione di $R$ e con gli stessi elementi neutri 0 e 1, un anello. Per verificare che un sottoinsieme $S$ di un anello $R$ è un sottoanello basta verificare che $0, 1 \in S$, che $(S, +, 0)$ è un sottogruppo di $(R, +, 0)$ e che $a, b \in S$ implica $ab \in S$.

**1.19 Esempio.** $\mathbb{Z}$ è un sottoanello di $\mathbb{Q}$. Il campo $\mathbb{Q}$ è un sottoanello di $\mathbb{R}$. Abbiamo le seguenti inclusioni di anelli:

$$\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C} \subset \mathbb{H}.$$

**1.20 Prodotti.** Siano $R_1$ e $R_2$ due anelli. Il *prodotto* $R_1 \times R_2$ *di* $R_1$ *per* $R_2$ è definito da

$$R_1 \times R_2 = \{(r, s) : r \in R_1 \text{ e } s \in R_2\}.$$

Con l'addizione data da $(r, s)+(r', s') = (r+r', s+s')$ e la moltiplicazione data da $(r, s)\cdot(r', s') = (r \cdot r', s \cdot s')$, il prodotto $R_1 \times R_2$ diventa un anello.

Se $R_1, R_2 \neq \{0\}$, il prodotto $R_1 \times R_2$ ha divisori di zero perché si ha

$$(r, 0) \cdot (0, s) = (0, 0) \qquad \text{per ogni } r \in R_1,\ s \in R_2.$$

**1.21 Esempio.** (*Anelli dei polinomi*) Sia $R$ un anello. Un *polinomio a coefficienti in* $R$ è una "espressione" del tipo

$$a_0 + a_1X + a_2X + \ldots + a_nX^n$$

dove $a_0, a_1, a_2, \ldots, a_n \in R$ e la lettera $X$ è soltanto un "simbolo". Gli elementi $a_i$ si dicono *i coefficienti* del polinomio. Equivalentemente, un polinomio è un'espressione

$$\sum_{i=0}^{\infty} a_iX^i$$

dove gli elementi $a_i$ appartengono ad $R$ e sono quasi tutti zero, cioè, esiste $n \in \mathbb{Z}_{\geq 0}$ tale che $a_i = 0$ per ogni $i > n$. Per definizione, due polinomi $\sum_{i=0}^{\infty} a_iX^i$ e $\sum_{i=0}^{\infty} b_iX^i$ sono uguali *se e soltanto se* $a_i = b_i$ per ogni $i \geq 0$.

Al posto di $X$ si utilizzano anche altre lettere, come $Y$, $Z$, $X_0$, $X_1$, etc. Di solito, non si scrivono gli zeri e si scrive $X$ per $1 \cdot X$ e $-aX^i$ per $(-a)X^i$. Spesso si scrive il polinomio in ordine opposto. Per esempio $Y^3 - 2Y + 1$ è il polinomio $1 + (-2) \cdot Y + 0 \cdot Y^2 + 1 \cdot Y^3$.

Il *grado* $\deg(f)$ (inglese: degree) di $f = \sum_{i=0}^{\infty} a_i X^i$ è il più grande indice $n$ tale che $a_n \neq 0$. Per *il polinomio zero* $0 = \sum_{i=0}^{\infty} 0 \cdot X^i$, il grado non è definito. Ogni tanto si trova $\deg(0) = -1$ oppure $\deg(0) = -\infty$. Un polinomio $f = \sum_{i=0}^{\infty} a_i X^i$ di grado $n$ si dice *monico* se $a_n = 1$.

Adesso introduciamo *l'anello* $R[X]$ *dei polinomi a coefficienti in* $R$:

$$R[X] = \left\{ \sum_{i=0}^{\infty} a_i X^i : a_i \in R \right\}$$

con l'addizione data da

$$\left( \sum_{i=0}^{\infty} a_i X^i \right) + \left( \sum_{i=0}^{\infty} b_i X^i \right) = \sum_{i=0}^{\infty} (a_i + b_i) X^i$$

e la moltiplicazione implicata dalle regole della distributività e da

$$(a_i X^i) \cdot (b_j X^j) = a_i b_j X^{i+j},$$

cioè

$$\left( \sum_{i=0}^{\infty} a_i X^i \right) \cdot \left( \sum_{i=0}^{\infty} b_i X^i \right) = \sum_{k=0}^{\infty} \Big( \sum_{\substack{i,j \\ i+j=k}} a_i b_j \Big) X^k.$$

Questa è la moltiplicazione di polinomi usuale; per esempio:

$$\begin{aligned} (5 - 3X^2) \cdot (3 + 4X + X^3) &= 5 \cdot (3 + 4X + X^3) - 3X^2 \cdot (3 + 4X + X^3) \\ &= 15 + 20X + 5X^3 - 9X^2 - 12X^3 - 3X^5 \\ &= 15 + 20X - 9X^2 - 7X^3 - 3X^5. \end{aligned}$$

Il polinomio $0 = \sum_{i=0}^{\infty} 0 \cdot X^i$ è l'elemento neutro per l'addizione e il polinomio $1 = 1 + 0 \cdot X + 0 \cdot X^2 + \ldots$ è l'identità di $R[X]$. Lasciamo al lettore la verifica che $R[X]$ è un anello.

L'anello $R[X]$ è commutativo se e soltanto se $R$ è commutativo. Si considera $R$ come il sottoanello dei polinomi *costanti* di $R[X]$: per $\alpha \in R$ si ha

$$\alpha = \alpha + 0 \cdot X + 0 \cdot X^2 + \ldots \in R[X].$$

Se $R$ è un dominio, anche $R[X]$ lo è (si veda l'Eserc.(1.L)). In questo caso il grado ha la seguente proprietà:

$$\deg(fg) = \deg(f) + \deg(g) \qquad \text{per ogni } f, g \in R[X] - \{0\}.$$

Induttivamente, si definisce *l'anello dei polinomi in* $n$ *variabili su* $R$:

$$R[X_1, X_2, \ldots, X_n] = (R[X_1, X_2, \ldots, X_{n-1}])[X_n].$$

Gli elementi di $R[X_1, X_2, \ldots, X_n]$ sono somme finite del tipo

$$\sum_{i_1=0}^{\infty}\sum_{i_2=0}^{\infty}\cdots\sum_{i_n=0}^{\infty} a_{i_1 i_2 \ldots i_n} X_1^{i_1} X_2^{i_2} \cdots X_n^{i_n}.$$

**1.22 Esempio importante.** (*Campi dei quozienti o delle frazioni).* Sia $R$ un dominio. A partire da $R$ costruiamo un campo $Q(R)$, detto il *campo quoziente di R.* Esso contiene $R$ ed "è generato da $R$" nel senso che ogni $x \in Q(R)$ ha la forma $xy^{-1}$ ,per certi $x, y \in R$.

Sia

$$\Omega = \{(a, r) \in R \times R : \ r \neq 0\}.$$

Innanzitutto, sull'insieme $\Omega$ definiamo una relazione *di equivalenza* mediante

$$(a, r) \sim (b, s) \quad \text{se e soltanto se} \quad as = br.$$

Verifichiamo che si tratta di una relazione di equivalenza: è facile vedere che $(a, r) \sim (a, r)$ e che $(a, r) \sim (b, s)$ se e soltanto se $(b, s) \sim (a, r)$. La relazione è dunque riflessiva e simmetrica. Per controllare la transitività utilizziamo la commutatività della moltiplicazione del dominio $R$: siano $(a, r) \sim (b, s)$ e $(b, s) \sim (c, t)$. Allora

$$ats = ast = brt = rbt = rcs = crs$$

e quindi $(at - cr)s = 0$. Siccome $s \neq 0$ ed $R$ è un dominio, troviamo $at = cr$, cioè $(a, r) \sim (c, t)$.

Definiamo adesso $Q(R)$ come l'insieme delle classi di equivalenza della relazione $\sim$ su $\Omega$. Scriveremo $\frac{a}{r}$ per la classe di $(a, r)$. Con questa notazione abbiamo

$$\frac{a}{r} = \frac{b}{s} \quad \text{se e soltanto se} \quad as = br.$$

Definiamo l'addizione e la moltiplicazione su $Q(R)$ mediante

$$\frac{a}{r} + \frac{b}{s} = \frac{as + br}{rs}, \qquad \frac{a}{r} \cdot \frac{b}{s} = \frac{ab}{rs}.$$

Si noti che $rs \neq 0$ perché $r, s \neq 0$ ed $R$ è un dominio.

Siccome l'addizione e la moltiplicazione sono definite in termini di rappresentanti delle classi di equivalenza, è necessario controllare che sono ben definite, cioè che la somma ed il prodotto non dipendono della scelta dei rappresentanti: supponiamo

$$\frac{a}{r} = \frac{a'}{r'} \quad \text{e} \quad \frac{b}{s} = \frac{b'}{s'},$$

cioè $ar' = a'r$ e $bs' = b's$. Abbiamo

$$\begin{aligned}(a's' + b'r')rs \ &= a's'rs + b'r'rs = (a'r)s's + (b's)r'r \\ &= ar's's + bs'r'r = (as + br)r's'\end{aligned}$$

e quindi, per definizione,

$$\frac{a's' + b'r'}{r's'} = \frac{as + br}{rs}.$$

Dunque l'addizione è ben definita. Similmente si controlla che la moltiplicazione è ben definita.

Lasciamo al lettore la verifica che, con questa addizione e moltiplicazione, $Q(R)$ è un *campo*. Per esempio, se $a \neq 0$, l'inverso moltiplicativo di $\frac{a}{r}$ è $\frac{r}{a}$. Consideriamo $R$ come sottoanello di $Q(R)$ identificando $a \in R$ con $\frac{a}{1}$.

Per l'anello $R = \mathbb{Z}$ si trova un campo isomorfo al campo $\mathbb{Q}$ dei numeri razionali. Se $K$ è un campo e $R = K[X]$ l'anello dei polinomi con coefficienti in $K$, allora $R$ è un dominio. Scriviamo $K(X)$ per il campo quoziente di $R$. Questo campo si dice *il campo delle funzioni razionali in una variabile su* $K$. Gli elementi di $K(X)$ hanno la forma

$$\frac{f(X)}{g(X)} \qquad \text{dove } f(X), g(X) \in K[X].$$

**1.23 Esempio.** (*Endomorfismi).* Sia $A$ un gruppo *additivo* e sia $\mathrm{End}(A)$ l'insieme degli endomorfismi di $A$ (ovvero degli omomorfismi di un gruppo in sé stesso). Per $f, g \in \mathrm{End}(A)$ definiamo la somma $f + g$ ed il prodotto $fg$:

$$(f+g)(a) = f(a) + g(a) \qquad \text{per ogni } a \in A, \qquad (fg)(a) = f(g(a)) \qquad \text{per ogni } a \in A.$$

Lasciamo al lettore la facile verifica che con quest'addizione e moltiplicazione $\mathrm{End}(A)$ diventa un anello; ossia *l'anello degli endomorfismi di* $A$. L'identità di $\mathrm{End}(A)$ è l'applicazione identica $\mathrm{Id}_A$.

Per esempio, se $A = \mathbb{R}^n$, ogni matrice $n \times n$ definisce un endomorfismo di $A$. Lasciamo al lettore la dimostrazione che $\mathrm{End}(\mathbb{Z}) = \mathbb{Z}$ ed è generato dall'identità $\mathrm{Id}_{\mathbb{Z}}$. Similmente si ha, per ogni intero positivo $n$ che $\mathrm{End}(\mathbb{Z}/n\mathbb{Z})$ è isomorfo a $\mathbb{Z}/n\mathbb{Z}$, generato dall'applicazione identica.

**1.24 Esempio.** (*Funzioni.*) Sia $X$ un insieme e sia $R$ un anello. L'insieme $R^X$ delle funzioni $X \longrightarrow R$ è un anello con le seguenti addizione e moltiplicazione: per $f, g : X \longrightarrow R$ definiamo

$$(f+g)(x) = f(x) + g(x), \qquad (f \cdot g)(x) = f(x) \cdot g(x),$$

dove l'addizione e la moltiplicazione a destra sono quelle di $R$.

Si ottengono esempi importanti di anelli se si considerano funzioni che hanno particolari proprietà. Per esempio, sia $X$ l'intervallo $[0,1] = \{x \in \mathbb{R} : 0 \leq x \leq 1\}$ e sia

$$C([0,1]) = \{f : [0,1] \longrightarrow \mathbb{R} : \ f \text{ è continua}\}.$$

Lasciamo al lettore la verifica che $C([0,1])$ è un sottoanello di $\mathbb{R}^{[0,1]}$. Altri esempi sono l'anello delle funzioni derivabili

$$C^1([0,1]) = \{f : [0,1] \longrightarrow \mathbb{R} : \ f \text{ è derivabile}\}.$$

e l'anello delle funzioni $C^\infty$:

$$C^\infty([0,1]) = \{f : [0,1] \longrightarrow \mathbb{R} : \ f \text{ è } \infty \text{ volte derivabile}\}.$$

## Esercizi.

(1.A) Sia $R$ un anello e sia $a \in R$. Dimostrare: se $ab = b$ per ogni $b \in R$ allora $a = 1$.

(1.B) Sia $2\mathbb{Z}$ l'insieme degli interi pari. Mostrare che con l'addizione e la moltiplicazione di $\mathbb{Z}$, l'insieme $2\mathbb{Z}$ soddisfa gli assiomi $(R_1)$, $(R_2)$ ed $(R_4)$, ma non $(R_3)$; $2\mathbb{Z}$ è un anello senza unitá

(1.C) Sia $R$ un anello.

(i) mostrare che per ogni $x \in R$ si ha $0 \cdot x = x \cdot 0 = 0$.

(ii) Sia $-1$ l'inverso additivo di $1 \in R$. Mostrare che $(-1) \cdot (-1) = 1$.

(iii) dimostrare le seguenti regole di calcolo: $(-1) \cdot a = -a$, $a \cdot (-b) = (-a) \cdot b = -(a \cdot b)$

(1.D) Sia $R$ un anello e sia $a \in R$ un'unità. Siano $b, c \in R$. Dimostrare che se $ba = ca$, allora $b = c$. Concludere che $a$ ha un unico inverso moltiplicativo.

(1.E) Sia $R$ un anello. Definiamo una nuova moltiplicazione $\star$ su $R$:

$$a \star b = ba.$$

mostrare che che, con l'addizione originale e la moltiplicazione nuova, $R$ è un anello. Questo anello si chiama *l'anello opposto di R.*

(1.F) Sia $R$ un anello e sia

$$Z(R) = \{a \in R : \ ax = xa \text{ per ogni } x \in R\}$$

il *centro* di $R$. Dimostrare che $Z(R)$ è un sottoanello di $R$.

(1.G) Sia $R$ un anello con la proprietà $x^3 = x$ per ogni $x \in R$. Dimostrare che $x + x + x + x + x + x = 0$ per ogni $x \in R$. Dare un esempio di un anello $R$ siffatto.

(1.H) (i) Sia $R$ un anello *finito*. Dimostrare che ogni $x \in R$ o è 0, o un divisore di zero oppure un'unità.

(ii) Dimostrare: un dominio di integrità finito è un anello di divisione.

(iii) Dare un esempio di un anello $R$ che contiene un elemento $a \neq 0$, il quale non è un'unità e non è un divisore di zero.

(iv) Dare un esempio di un anello infinito con divisori di zero.

(1.I) Sia $\mathbb{Z}[i]$ l'anello degli interi di Gauss. Siano $a, b \in \mathbb{Z}$ e sia $z = a + bi \in \mathbb{Z}[i]$. mostrare che $z$ è un'unità se e soltanto se $a^2 + b^2 = 1$. Calcolare $\mathbb{Z}[i]^*$.

(1.J) Sia $H$ il sottoinsieme dell'insieme dei quaternioni $\mathbb{H}$ dato da

$$H = \{a + bi + cj + dk : a, b, c, d \in \mathbb{Z}\}.$$

Dimostrare che $H$ è un anello non commutativo. Dimostrare che $H$ non contiene divisori di 0.

(1.K) Sia $m \in \mathbb{Z}$. Supponiamo che $m \in \mathbb{Z}$ non sia un quadrato.

(i) Dimostrare che l'insieme

$$\mathbb{Z}[\sqrt{m}] = \{a + b\sqrt{m} : \ a, b \in \mathbb{Z}\}$$

è un sottoanello di $\mathbb{C}$.

(ii) Sia $m = 7$. Trovare un'unità $\varepsilon \neq \pm 1$ nell'anello $\mathbb{Z}[\sqrt{7}]$. (Sugg. Verificare che $a+b\sqrt{7}$ è un'unità se e soltanto se $(a + b\sqrt{7})(a - b\sqrt{7}) = a^2 - 7b^2$ è uguale a $\pm 1$.)

(iii) Trovare una infinità di soluzioni intere dell'equazione $a^2 - 7b^2 = 1$

(iv) Dimostrare che, in realtà, non può mai essere $a^2 - 7b^2 = -1$

(1.L) Sia $R$ un anello senza divisori di zero.

(i) Dimostrare che neanche $R[X]$ ha divisori di zero.

(ii) Siano $f, g \in R[X]$ polinomi non nulli. mostrare che che

$$\deg(f) + \deg(g) = \deg(fg).$$

(1.M) (i) Sia $R$ un anello senza divisori di zero. Dimostrare che $R[X]^* = R^*$.

(ii) mostrare che $\overline{1} + \overline{5}X \in (\mathbb{Z}/25\mathbb{Z})[X]$ è un'unità.

(1.N) Siano $R_1$ e $R_2$ anelli.

(i) Dimostrare che

$$(R_1 \times R_2)^* = R_1^* \times R_2^*.$$

(ii) Dimostrare: se $R_1 \times R_2$ è un dominio di integrità, allora uno degli anelli $R_1, R_2$ è l'anello banale.

# 2 Omomorfismi ed ideali

In questo paragrafo introduciamo gli omomorfismi di anelli. Le immagini di omomorfismi sono sempre sottoanelli, ma i nuclei sono *ideali*. Studiamo quindi il concetto importante di *ideale* di un anello, introdotto dal matematico tedesco E. E. Kummer nel 1845.

**2.1 Definizione.** Siano $R_1, R_2$ due anelli. Un *omomorfismo (di anelli)* da $R_1$ a $R_2$ è una mappa

$$f : R_1 \longrightarrow R_2$$

che soddisfa

$$\begin{array}{rll} f(a+b) & = f(a) + f(b) & \text{per ogni } a, b \in R_1, \\ f(ab) & = f(a)f(b) & \text{per ogni } a, b \in R_1, \\ f(1) & = 1. & \end{array}$$

La richiesta che $f(1) = 1$ non sarebbe strettamente necessaria, viene qui imposta per uniformità con la teoria dei gruppi, e per assicurare che l'immagine di un omomorfismo sia un sottoanello di $R_2$. Se l'omomorfismo è suriettivo, oppure se $R_2$ non ha divisori dello zero è automaticamente vera (verificare!).

Un omomorfismo biiettivo si dice un *isomorfismo* o anche, se $R_1 = R_2$, un *automorfismo*. L'insieme

$$\ker(f) = \{x \in R_1 : f(x) = 0\}$$

si dice il *nucleo di* $f$.

**2.2 Esempio.**

(*i*) Sia $n$ un intero positivo. L'applicazione canonica

$$\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}, \qquad a \longmapsto a \bmod n$$

è un omomorfismo dall'anello $\mathbb{Z}$ all'anello $\mathbb{Z}/n\mathbb{Z}$.

(*ii*) Sia $\alpha \in \mathbb{R}$. L'applicazione

$$\Phi : \mathbb{R}[X] \longrightarrow \mathbb{R}, \qquad f \longmapsto f(\alpha)$$

è un omomorfismo di anelli. Lasciamo la verifica al lettore. È facile vedere che $\Phi$ è un omomorfismo suriettivo. In generale, per ogni anello *commutativo* $R$ ed ogni $\alpha \in R$, l'applicazione $\Phi : R[X] \longrightarrow R$ data da $\Phi(f) = f(\alpha)$ è un omomorfismo. Questo non è più vero per anelli non commutativi. Si veda l'Eserc.(2.H).

(*iii*) Sia $R$ un anello e sia $R'$ un sottoanello di $R$. Allora l'inclusione $R' \hookrightarrow R$ è un omomorfismo di anelli.

(*iv*) Siano $R_1$ e $R_2$ due anelli. La *proiezione*

$$\pi_1 : R_1 \times R_2 \longrightarrow R_1$$

data da $\pi_1(r, s) = r$ è un omomorfismo. Anche l'altra proiezione $\pi_2 : R_1 \times R_2 \longrightarrow R_2$ data da $\pi_2(r, s) = s$ è un omomorfismo.

(*v*) Sia $R$ un anello. L'applicazione $\mathbb{Z} \longrightarrow R$ data da $m \mapsto m$, cioè

$$m \longmapsto \begin{cases} \underbrace{1+1+\cdots+1}_{m \text{ volte}}; & \text{se } m > 0, \\ \underbrace{-1-1-\cdots-1}_{-m \text{ volte}}; & \text{se } m < 0. \\ 0; & \text{se } m = 0, \end{cases}$$

è un omomorfismo. Si controlli che questa applicazione è l'unico omomorfismo da $\mathbb{Z}$ a $R$.

**2.3 Definizione.** Sia $R$ un anello. Un sottoinsieme $I \subset R$ si dice un *ideale sinistro di* $R$ se $I$ è un sottogruppo additivo di $R$ con la proprietà

$$ra \in I \qquad \text{per ogni } r \in R \text{ ed ogni } a \in I.$$

Un sottoinsieme $I \subset R$ si dice un *ideale destro di* $R$ se $I$ è un sottogruppo additivo di $R$ con la proprietà

$$ar \in I \qquad \text{per ogni } r \in R \text{ ed ogni } a \in I.$$

Un *ideale (bilaterale)* è un ideale sia sinistro, sia destro di $R$.

**2.4 Esempi.**

(*i*) (*Ideali banali*) Ogni anello $R$ possiede i cosidetti ideali *banali* $\{0\}$ e $R$.

(*ii*) (*Nuclei*) Sia $f : R_1 \longrightarrow R_2$ un omomorfismo. Allora, il nucleo di $f$ è un ideale di $R_1$. Infatti il nucleo di $f$ è un sottogruppo additivo di $R$. Per vedere che $\ker(f)$ è un ideale di $R$ prendiamo $r \in R$ e $x \in I$. Abbiamo $f(rx) = f(r)f(x) = f(r) \cdot 0 = 0$ e dunque $rx \in I$. Similmente si dimostra che $xr \in I$.

Un omomorfismo $f$ di anelli è iniettivo se e soltanto se il nucleo di $f$ è zero. Questo fatto segue dal risultato corrispondente per i gruppi.

(*iii*) (*Ideali principali*) Sia $R$ un anello e sia $x \in R$. L'insieme

$$Rx = \{rx : r \in R\}$$

è un ideale sinistro di $R$. Similmente $xR = \{xr : r \in R\}$ è un ideale destro di $R$. Se $R$ è commutativo gli ideali $xR$ e $Rx$ coincidono. Questo ideale si dice *l'ideale generato da* $x$ e si scrive anche $(x)$. Gli ideali di $R$ generati da un *unico* elemento di $R$ si dicono *ideali principali*.

(*iv*) Sia $I$ un ideale di $\mathbb{Z}$. Questo significa, in particolare, che $I$ è un sottogruppo additivo di $\mathbb{Z}$. Ogni sottogruppo di $\mathbb{Z}$ ha la forma $d\mathbb{Z}$. Ogni ideale di $\mathbb{Z}$ è dunque principale. Ogni sottogruppo di $\mathbb{Z}$ è quindi anche un ideale di $\mathbb{Z}$.

(*v*) Sia $R$ un anello commutativo e siano $a_1$, $a_2, \ldots,$ $a_n$ elementi di $R$. Scriviamo $a_1R + a_2R + \cdots + a_nR$ oppure $(a_1, a_2, \ldots, a_n)$ per *l'ideale $I$ generato da $a_1, a_2, \ldots, a_n$*. L'ideale $I$ è definito da

$$I = \{x_1a_1 + x_2a_2 + \cdots + x_na_n : x_1, x_2, \ldots, x_n \in R\}.$$

L'ideale $I$ è il più piccolo ideale di $R$ che contiene gli elementi $a_1$, $a_2, \ldots,$ $a_n$.

**2.5 Esempio.** Per esempio consideriamo l'ideale $I = (2, X)$ generato dagli elementi 2 ed $X$ nell'anello $\mathbb{Z}[X]$. L'ideale $I$ non è principale. Per dimostrare questo fatto, supponiamo che $I = (f)$ per un certo polinomio $f \in \mathbb{Z}[X]$. Dunque

$$2 = h \cdot f, \qquad X = g \cdot f,$$

per certi polinomi $h, g \in \mathbb{Z}[X]$. Siccome $\mathbb{Z}$ è un dominio di integrità, il grado deg è additivo: $\deg(f) + \deg(h) = \deg(2) = 0$. Siccome $\deg(f) \geq 0$, abbiamo $\deg(f) = 0$, cioè $f$ è un polinomio costante. Similmente, $g$ è un polinomio di grado 1. Siccome $X = g \cdot f$, abbiamo, per un certo $\alpha \in \mathbb{Z}$, che $g = X + \alpha$ e $f = 1$ oppure $g = -X + \alpha$ e $f = -1$. In ogni caso troviamo che $1 \in I$, il che è impossibile perché $I$ consiste di polinomi $\sum_{k\geq 0} a_kX^k$ con $a_0$ pari. Concludiamo che $I = (2, X)$ non è un ideale principale.

**2.6 Proposizione.** Sia $R$ un anello e sia $I \subset R$ un ideale di $R$. Se $I$ contiene un'unità, allora $I = R$.

**Dimostrazione.** Sia $a \in R^*$ in $I$. Allora $1 = a \cdot a^{-1} \in I$ e dunque $x = x \cdot 1 \in I$ per ogni $x \in R$. In altre parole $I = R$, come richiesto. □

**2.7 Corollario.** Sia $R$ un anello con divisione.

(*i*) I soli ideali di $R$ sono quelli banali.

(*ii*) Sia $R'$ un anello non banale e sia $f : R \longrightarrow R'$ un omomorfismo. Allora $f$ è iniettivo.

**Dimostrazione.** *(i)* Ogni elemento $x \neq 0$ di $R$ è un unità. L'anello $R$ ha quindi per la Prop.2.6 soltanto i due ideali $\{0\}$ e $R$.
*(ii)* Siccome $f(1) = 1$, l'elemento 1 non è contenuto nel nucleo di $f$. Dunque l'ideale $\ker(f)$ non è uguale a $R$ e per la prima parte abbiamo $\ker(f) = 0$, come richiesto. □

**2.8 Somme, prodotti e intersezioni di ideali.** Sia $R$ un anello e siano $I$, $J$ ideali bilaterali di $R$. È facile vedere che l'intersezione $I \cap J$ è un ideale di $R$. L'ideale $I \cap J$ è il più grande ideale contenuto sia in $I$, sia in $J$. L'unione di $I$ e $J$ non è, in generale, un ideale.

La *somma $I + J$ di $I$ e $J$* è definita da

$$I + J = \{x + y : x \in I \text{ ed } y \in J\}.$$

Lasciamo al lettore la verifica che si tratta di un ideale. Ovviamente $I + J$ contiene gli ideali $I$ e $J$. D'altra parte, ogni ideale che contiene $I$ e $J$ contiene anche la somma $I + J$. Dunque,

$I+J$ è il più piccolo ideale di $R$ che contiene sia $I$ che $J$. Si dice che $I$ e $J$ sono *coprimi* oppure che *non hanno divisori comuni,* se $I+J=R$.

Il *prodotto* $IJ$ *di* $I$ *e* $J$ è definito da

$$IJ=\left\{\sum_{k=1}^{m} x_k y_k : m\in\mathbb{Z}_{>0},\quad x_k\in I,\, y_k\in J\right\}.$$

Lasciamo al lettore la verifica che $IJ$ è un ideale di $R$. In generale, l'insieme $\{xy : x\in I, y\in J\}$ non è un ideale. L'ideale $IJ$ è contenuto in sia $I$ che $J$ e quindi $IJ\subset I\cap J$. Abbiamo il seguente diagramma di ideali di $R$:

$$\begin{array}{ccccccc} & & & & I & & \\ & & & \subset & & \subset & \\ IJ & \subset & I\cap J & & & & I+J \quad \subset \quad R \\ & & & \subset & & \subset & \\ & & & & J & & \end{array}$$

**2.9 Esempio.** Adesso vediamo che significato hanno questi ideali nel caso $R=\mathbb{Z}$. Siano $I, J$ due ideali di $\mathbb{Z}$. Siccome ogni ideale di $\mathbb{Z}$ è principale, possiamo scrivere $I=n\mathbb{Z}$ e $J=m\mathbb{Z}$ per certi interi $n$, $m$.

L'intersezione $n\mathbb{Z}\cap m\mathbb{Z}$ consiste degli interi $a$ che sono divisibili sia per $n$, sia per $m$. Dunque il *minimo comune multiplo* $\mathrm{mcm}(n,m)$ di $n$ ed $m$ è contenuto nella intersezione $n\mathbb{Z}\cap m\mathbb{Z}$. D'altra parte, ogni multiplo comune di $n$ ed $m$ è divisibile per $\mathrm{mcm}(n,m)$. Concludiamo che

$$n\mathbb{Z}\cap m\mathbb{Z}=\mathrm{mcm}(n,m)\mathbb{Z}.$$

La somma $n\mathbb{Z}+m\mathbb{Z}$ è, per definizione, uguale all'insieme $\{an+bm : a,b\in\mathbb{Z}\}$. Esso contiene $\mathrm{mcd}(n,m)$. È banale che ogni numero della forma $an+bm$ è divisibile per $\mathrm{mcd}(n,m)$. Concludiamo che

$$n\mathbb{Z}+m\mathbb{Z}=\mathrm{mcd}(n,m)\mathbb{Z}.$$

In particolare, $\mathrm{mcd}(n,m)=1$ se e soltanto se $n\mathbb{Z}+m\mathbb{Z}=\mathbb{Z}$. Questo spiega perché si dice che due ideali $I$, $J$ di un anello arbitrario $R$, sono coprimi, oppure non hanno divisori comuni, quando $I+J=R$.

Il prodotto di $n\mathbb{Z}$ e $m\mathbb{Z}$ è dato da

$$(n\mathbb{Z})(m\mathbb{Z})=nm\mathbb{Z}.$$

**2.10 Definizione.** (*Anelli quoziente*). Sia $R$ un anello e sia $I$ un ideale di $R$. Se consideriamo soltanto la struttura *additiva,* vediamo che $R$ è un gruppo abeliano e $I$ un sottogruppo normale di $R$. Dunque è definito il quoziente $R/I$. Come solito, scriviamo $\overline{x}$ per la classe laterale $x+I$ dell'elemento $x\in R$. Si ha $\overline{x}=\overline{y}$ se e soltanto se $x-y\in I$.

Per due elementi $\overline{x},\overline{y}\in R/I$ definiamo

$$\overline{x}\cdot\overline{y}=\overline{xy}.$$

Con questa moltiplicazione $R/I$ diventa un anello, *l'anello quoziente di $R$ per $I$*. Verifichiamo prima che la moltiplicazione è ben definita. Prendiamo $x,\, x' \in R$ e $y,\, y' \in R$ tali che $\overline{x} = \overline{x'}$ e $\overline{y} = \overline{y'}$. Dunque

$$x' = x + a \qquad \text{e} \qquad y' = y + b \qquad \text{per certe } a,\, b \in I$$

e, per la distributività di $R$,

$$x'y' = xy + xb + ay + ab.$$

Siccome $I$ è un ideale, gli elementi $xb$, $ay$ e $ab$ sono tutti in $I$. Concludiamo che

$$\overline{x'y'} = \overline{xy}$$

e quindi la moltiplicazione è ben definita.

È molto facile verificare gli assiomi di anello per $R/I$: abbiamo già detto che vale $(R_1)$. L'assioma $(R_2)$ vale perché

$$(\overline{x}\,\overline{y})\overline{z} = \overline{xy}\,\overline{z} = \overline{(xy)z} = \overline{x(yz)} = \overline{x}\,\overline{yz} = \overline{x}(\overline{y}\,\overline{z})$$

per ogni $\overline{x}, \overline{y}, \overline{z} \in R/I$.

L'elemento $\overline{1}$ è l'identità dell'anello $R/I$ e la distributività vale. Dunque, valgono anche gli assiomi $(R_3)$ e $(R_4)$.

**2.11 Proposizione.** Sia $I$ un ideale di un anello $R$. L'omomorfismo canonico

$$\pi : R \longrightarrow R/I, \qquad x \longmapsto \overline{x}$$

è un omomorfismo suriettivo. Il nucleo di $\pi$ è $I$.

**Dimostrazione.** Siccome $\pi(x) = \overline{x}$, la mappa $\pi$ è suriettiva. Abbiamo $x \in \ker(\pi)$ se e soltanto se $\pi(x) = \overline{x} = \overline{0}$. Questo è equivalente a $x \in I$, come richiesto. □

## Esercizi.

(2.A) Sia $f : R_1 \longrightarrow R_2$ un omomorfismo. Mostrare che l'immagine di $f$ è un sottoanello di $R_2$.

(2.B) Sia $R$ un anello. Mostrare che esiste unico un omomorfismo di anelli $\mathbb{Z} \longrightarrow R$. Mostrare che esiste unico un omomorfismo di anelli $R \longrightarrow \{0\}$.

(2.C) (i) Sia $f : \mathbb{Q} \longrightarrow \mathbb{Q}$ un omomorfismo di anelli. mostrare che $f$ è l'applicazione identica.

(ii) Sia $f : \mathbb{R} \longrightarrow \mathbb{R}$ un omomorfismo. mostrare che $f(x) > 0$ se $x > 0$.

(iii) Sia $f : \mathbb{R} \longrightarrow \mathbb{R}$ un omomorfismo. mostrare che $f$ è l'applicazione identica.

(2.D) mostrare che esiste un omomorfismo di anelli $f : \mathbb{C} \longrightarrow \mathbb{C}$ distinto dall'applicazione identica.

(2.E) Sia $f : R \longrightarrow R'$ un omomorfismo di anelli.

(i) Dimostrare che $f$ manda $R^*$ in $R'^*$ e l'applicazione $f^* : R^* \longrightarrow R'^*$, data da $f^*(\varepsilon) = f(\varepsilon)$, è un omomorfismo di gruppi.

(ii) mostrare: $f^*$ è iniettivo se $f$ è iniettivo.

(iii) È vero che $f^*$ è suriettivo se $f$ è suriettivo?

(2.F) Siano $R_1$ ed $R_2$ due anelli.

(i) Siano $I_1 \subset R_1$ e $I_2 \subset R_2$ ideali. mostrare che $I_1 \times I_2$ è un ideale di $R_1 \times R_2$.

(ii) Dimostrare che ogni ideale $I \subset R_1 \times R_2$ ha la forma $I = I_1 \times I_2$ dove $I_1 \subset R_1$ e $I_2 \subset R_2$ sono ideali.

(2.G) Sia $R$ un anello e siano $I, J \subset R$ due ideali di $R$. mostrare: $I \cup J$ è un ideale se e soltanto se $I \subset J$ o $J \subset I$.

(2.H) Sia $R$ un anello. Sia $F_\alpha : R[X] \longrightarrow R$ l'applicazione data da $f \mapsto f(\alpha)$.

(i) mostrare che $F_\alpha$ è un omomorfismo di anelli se $\alpha$ è contenuto nel centro di $R$. (Si veda l'Eserc.(1.F)).

(ii) Dimostrare: la mappa $F_\alpha$ è un omomorfismo per ogni $\alpha \in R$ se e soltanto se $R$ è commutativo.

(2.I) Sia $R$ un anello. mostrare che

$$I = \left\{ \sum_{k=0}^{\infty} a_k X^k \in R[X] : \; a_0 = a_1 = a_2 = 0 \right\}$$

è un ideale di $R[X]$ e che $I = (X^3)$.

(2.J) Sia $A$ un gruppo abeliano. Mostrare che

$$\{f \in \mathrm{End}(A) : \; f(a) = 0 \text{ se } a \in A \text{ ha ordine finito}\}$$

è un ideale di $\mathrm{End}(A)$.

(2.K) (i) mostrare che la mappa $\Psi : \mathbb{Z}[X] \longrightarrow \mathbb{Z}/2\mathbb{Z}$ data da $f \mapsto f(0) \bmod 2$ è un omomorfismo suriettivo.

(ii) mostrare che $\ker(\Psi)$ è l'ideale $(2, X)$.

(iii) Dimostrare che

$$\mathbb{Z}[X]/(2, X) \cong \mathbb{Z}/2\mathbb{Z}.$$

(2.L) Sia $R$ un anello e supponiamo che l'applicazione $f : R \longrightarrow R$ data da $f(x) = x^2$ sia un omomorfismo di anelli.

(i) mostrare che $R$ è un anello commutativo.

(ii) mostrare che per ogni $x \in R$ si ha $x + x = 0$.

(iii) Dimostrare: se $x \in \ker(f)$, allora $1 + x \in R^*$.

(2.M) (*Numeri duali.*) Sia $R$ un anello commutativo. *L'anello* $R[\varepsilon]$ *dei numeri duali su* $R$ consiste delle espressioni $a + b\varepsilon$ con $a, b \in R$. L'addizione e moltiplicazione sono definite da

$$\begin{aligned}(a + b\varepsilon) + (c + d\varepsilon) &= (a + c) + (b + d)\varepsilon,\\ (a + b\varepsilon) \cdot (c + d\varepsilon) &= (ac) + (ad + bc)\varepsilon.\end{aligned}$$

(i) Mostrare che $\varepsilon^2 = 0$. Questa formula e le leggi della distributività implicano la formula generale per la moltiplicazione data sopra.

(ii) Dimostrare $R[\varepsilon] \cong R[X]/(X^2)$.

(iii) Se $R$ è un campo, allora l'anello $R[\varepsilon]$ ha esattamente tre ideali distinti.

(iv) Sia $R$ un campo. Mostrare che c'è un isomorfismo di gruppi

$$R[\varepsilon]^* \cong R^* \times R.$$