Anelli, ideali e quozienti

Gabriel Antonio Videtta

31 dicembre 2022

Indice

1 Anelli e prime proprietà

Definizione 1.1. Si definisce **anello**[1] una struttura algebrica costruita su un insieme A e due operazioni binarie $+$ e $\cdot$[2] avente le seguenti proprietà:

- $(A, +)$ è un *gruppo abeliano*, alla cui identità, detta *identità additiva*, ci si riferisce con il simbolo 0,
- $\forall\, a, b, c \in A,\ (ab)c = a(bc)$,
- $\forall\, a, b, c \in A,\ (a + b)c = ac + bc$,
- $\forall\, a, b, c \in A,\ a(b + c) = ab + ac$,
- $\exists 1 \in A \mid \forall\, a \in A,\ 1a = a = a1$, e tale 1 viene detto *identità moltiplicativa*.

Come accade per i gruppi, gli anelli soddisfano alcune proprietà algebriche particolari, tra le quali si citano le più importanti:

Proposizione 1.1. $\forall\, a \in A,\ 0a = 0 = a0$.

Dimostrazione. $0a = (0 + 0)a = 0a + 0a \implies 0a = 0$. Analogamente $a0 = a(0 + 0) = a0 + a0 \implies a0 = 0$. □

Proposizione 1.2. $\forall\, a \in A,\ -(-a) = a$.

Dimostrazione. $-(-a) - a = 0 \wedge a - a = 0 \implies -(-a) = a$, per la proprietà di unicità dell'inverso in un gruppo[3]. □

[1] In realtà, si parla in questo caso di anello *con unità*, in cui vale l'assioma di esistenza di un'identità moltiplicativa. In questo documento si identificherà con "anello" solamente un anello con unità.

[2] D'ora in avanti il punto verrà omesso.

[3] In questo caso, il gruppo additivo dell'anello.

Proposizione 1.3. $a(-b) = (-a)b = -(ab)$.

Dimostrazione. $a(-b) + ab = a(b-b) = a0 = 0 \implies a(-b) = -(ab)$, per la proprietà di unicità dell'inverso in un gruppo. Analogamente $(-a)b + ab = (a-a)b = 0b = 0 \implies (-a)b = -(ab)$. □

Corollario 1.1. $(-1)a = a(-1) = -a$.

Proposizione 1.4. $(-a)(-b) = ab$.

Dimostrazione. $(-a)(-b) = -(a(-b)) = -(-(ab)) = ab$, per la *Proposizione 1.3.* □

Si enuncia invece adesso la nozione di **sottoanello**, in tutto e per tutto analoga a quella di *sottogruppo*.

Definizione 1.2. Si definisce sottoanello rispetto all'anello A un anello B avente le seguenti proprietà:

- $B \subseteq A$,
- $0, 1 \in B$,
- $\forall\, a, b \in B,\ a + b \in B \wedge ab \in B$.

Definizione 1.3. Un sottoanello B rispetto ad A si dice **proprio** se $B \neq A$.

Definizione 1.4. Un anello si dice **commutativo** se $\forall\, a,\ b \in A,\ ab = ba$.

Esempio 1.1. Un facile esempio di anello commutativo è $\mathbb{Z}/n\mathbb{Z}$.

Definizione 1.5. Un elemento a di un anello A si dice **invertibile** se $\exists\, b \in A \mid ab = ba = 1$.

Definizione 1.6. Dato un anello A, si definisce A^* come l'insieme degli elementi invertibili di A, che a sua volta forma un *gruppo moltiplicativo*.

Definizione 1.7. Un anello A si dice **corpo** se $\forall\, a \neq 0 \in A,\ \exists\, b \in A \mid ab = ba = 1$, ossia se $A \setminus \{0\} = A^*$.

Esempio 1.2. L'esempio più rilevante di corpo è quello dei *quaternioni* $\mathbb{H}$, definiti nel seguente modo:

$$\mathbb{H} = \{a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k} \mid a,\, b,\, c,\, d \in \mathbb{R}\},$$

dove:

$$\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = -1, \quad \mathbf{ij} = \mathbf{k},\, \mathbf{jk} = \mathbf{i},\, \mathbf{ki} = \mathbf{j}.$$

Infatti ogni elemento non nullo di $\mathbb{H}$ possiede un inverso moltiplicativo:

$$(a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k})^{-1} = \frac{a - b\mathbf{i} - c\mathbf{j} - d\mathbf{k}}{a^2 + b^2 + c^2 + d^2},$$

mentre la moltiplicazione non è commutativa.

Definizione 1.8. Un anello commutativo che è anche un corpo si dice **campo**.

Esempio 1.3. Alcuni campi, tra i più importanti, sono $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ e $\mathbb{Z}/p\mathbb{Z}$ con p primo.

Definizione 1.9. Un elemento $a \neq 0$ appartenente a un anello A si dice **divisore di zero** se $\exists\, b \neq 0 \in A \mid ab = 0$ o $ba = 0$.

Esempio 1.4. 2 è un divisore di zero in $\mathbb{Z}/6\mathbb{Z}$, infatti $2 \cdot 3 \equiv 0 \pmod 6$.

Definizione 1.10. Un anello commutativo in cui non sono presenti divisori di zero si dice **dominio d'integrità**, o più semplicemente *dominio*.

Proposizione 1.5 (*Legge di annullamento del prodotto*)**.** Sia D un dominio. Allora $ab = 0 \implies a = 0 \vee b = 0$.

Dimostrazione. Siano $a, b \in D \mid ab = 0$. Se $a = 0$, la condizione è soddisfatta. Se invece $a \neq 0$, b deve essere per forza nullo, altrimenti si sarebbe trovato un divisore di 0, e D non sarebbe un dominio, ↯. □

Esempio 1.5. L'anello dei polinomi su un campo, $\mathbb{K}[x]$, è un dominio.

2 Omomorfismi di anelli e ideali

Definizione 2.1. Un **omomorfismo di anelli**[4] è una mappa $\phi : A \to B$ – con A e B anelli – soddisfacente alcune particolari proprietà:

- ϕ è un *omomorfismo di gruppi* rispetto all'addizione di A e di B, ossia $\forall\, a, b \in A$, $\phi(a + b) = \phi(a) + \phi(b)$,
- $\phi(ab) = \phi(a)\phi(b)$,
- $\phi(1_A) = 1_B$.

Definizione 2.2. Se $\phi : A \to B$ è un omomorfismo iniettivo, si dice che ϕ è un **monomorfismo**.

Definizione 2.3. Se $\phi : A \to B$ è un omomorfismo suriettivo, si dice che ϕ è un **epimorfismo**.

Definizione 2.4. Se $\phi : A \to B$ è un omomorfismo bigettivo[5], si dice che ϕ è un **isomorfismo**.

Prima di enunciare l'analogo del *Primo teorema d'isomorfismo* dei gruppi in relazione agli anelli, si rifletta su un esempio di omomorfismo:

Esempio 2.1. Sia $\phi : \mathbb{Z} \to \mathbb{Z}, k \mapsto 2k$ un omomorfismo. Esso è un monomorfismo, infatti $\phi(x) = \phi(y) \implies 2x = 2y \implies x = y$. Pertanto $\operatorname{Ker}\phi = \{0\}$. Sebbene $\operatorname{Ker}\phi < \mathbb{Z}$, esso **non è un sottoanello**[6].

Dunque, con lo scopo di definire meglio le proprietà di un *kernel*, così come si introdotto il concetto di *sottogruppo normale* per i gruppi, si introduce ora il concetto di **ideale**.

[4] La specificazione "di anelli" è d'ora in avanti omessa.
[5] Ovvero se è sia un monomorfismo che un epimorfismo.
[6] Infatti $1 \notin \operatorname{Ker}\phi$.

Definizione 2.5. Si definisce ideale rispetto all'anello A un insieme I avente le seguenti proprietà:

- $I \leq A$,
- $\forall\, a \in A$, $\forall\, b \in I$, $ab \in I$ e $ba \in I$.

Esempio 2.2. Sia I l'insieme dei polinomi di $\mathbb{R}[x]$ tali che 2 ne sia radice. Esso altro non è che un ideale, infatti $0 \in I \wedge \forall\, f(x), g(x) \in I, (f+g)(2) = 0$ (i.e. $I < \mathbb{R}[x]$) e $\forall\, f(x) \in A$, $g(x) \in I$, $(fg)(2) = 0$.

Proposizione 2.1. Sia I un ideale di A. $1 \in I \implies I = A$.

Dimostrazione. Per le proprietà dell'ideale I, $\forall\, a \in A$, $a1 = a \in I \implies A \subseteq I$. Dal momento che anche $I \subseteq A$, si deduce che $I = A$. □

Proposizione 2.2. Sia $\phi : A \to B$ un omomorfismo. $\operatorname{Ker}\phi$ è allora un ideale di A.

Dimostrazione. Poiché ϕ è anche un omomorfismo tra gruppi, si deduce che $\operatorname{Ker}\phi \leq A$. Inoltre $\forall\, a \in A$, $\forall\, b \in \operatorname{Ker}\phi$, $\phi(ab) = \phi(a)\phi(b) = \phi(a)0 = 0 \implies ab \in I$. □

Proposizione 2.3. Sia $\phi : A \to B$ un omomorfismo. $\operatorname{Imm}\phi$ è allora un sottoanello di B.

Dimostrazione. Chiaramente $0, 1 \in \operatorname{Imm}\phi$, dal momento che $\phi(0) = 0$, $\phi(1) = 1$. Inoltre, dalla teoria dei gruppi, si ricorda anche che $\operatorname{Imm}\phi \leq B$. Infine, $\forall\, \phi(a)$, $\phi(b) \in \operatorname{Imm}\phi$, $\phi(a)\phi(b) = \phi(ab) \in \operatorname{Imm}\phi$. □

Definizione 2.6. Si definisce con la notazione (a) l'ideale *bilatero* generato da a in A, ossia:

$$(a) = \{ba \mid b \in A\} \cup \{ab \mid b \in A\}.$$

Definizione 2.7. Si dice che un ideale I è *principale* o **monogenerato**, quando $\exists\, a \in I \mid I = (a)$.

Esempio 2.3. In relazione all'*Esempio 2.2*, l'ideale I è monogenerato[7]. In particolare, $I = (x - 2)$.

3 Anelli quoziente e teorema d'isomorfismo

Si definisce invece adesso il concetto di **anello quoziente**, in modo completamente analogo a quello di *gruppo quoziente*:

Definizione 3.1. Sia A un anello e I un suo ideale, si definisce A/I l'anello ottenuto quozientando A per I. Gli elementi di tale anello sono le classi di equivalenza di $\sim$ (i.e. gli elementi di $A/\!\sim$), dove $\forall\, a, b \in A$, $a \sim b \iff a - b \in I$. Tali classi di equivalenza vengono indicate come $a+I$, dove a è un rappresentante della classe. L'anello è così dotato di due operazioni:

[7] Non è un caso: $\mathbb{R}[x]$, in quanto anello euclideo, si dimostra essere un PID (*principal ideal domain*), ossia un dominio che ammette *solo* ideali monogenerati.

- $\forall\, a,\, b \in A,\, (a+I)+(b+I) = (a+b)+I$,
- $\forall\, a,\, b \in A,\, (a+I)(b+I) = ab+I$.

Osservazione. L'addizione di A/I è ben definita, dal momento che $I \trianglelefteq A$, in quanto sottogruppo di un gruppo abeliano.

Osservazione. Anche la moltiplicazione di A/I è ben definita. Siano $a \sim a'$, $b \sim b'$ quattro elementi di A tali che $a = a' + i_1$ e $b = b' + i_2$ con $i_1,\, i_2 \in I$. Allora $ab = (a'+i_1)(b'+i_2) = a'b' + \underbrace{i_1b' + i_2a' + i_1i_2}_{\in I} \implies ab \sim a'b'$.

Proposizione 3.1. $A/\{0\} \cong A$.

Dimostrazione. Sia $\pi : A \to A/\{0\}$, $a \mapsto a + \{0\}$ l'omomorfismo di proiezione al quoziente. Innanzitutto, $a \sim a' \iff a - a' = 0 \iff a = a'$, per cui π è un monomorfismo (altrimenti si troverebbero due $a,\, b \mid a \neq b \wedge a \sim b$). Infine, π è un epimorfismo, dal momento che $\forall\, a + \{0\} \in A/\{0\}$, $\pi(a) = a + \{0\}$. Pertanto π è un isomorfismo. □

Adesso è possibile enunciare il seguente fondamentale teorema:

Teorema 3.1 (*Primo teorema d'isomorfismo*)**.** Sia $\phi : A \to B$ un omomorfismo. $A/\operatorname{Ker}\phi \cong \operatorname{Imm}\phi$.

Dimostrazione. La dimostrazione procede in modo analogo a quanto visto per il teorema correlato in teoria dei gruppi.

Sia $\zeta : A/\operatorname{Ker}\phi \to \operatorname{Imm}\phi$, $a + \operatorname{Ker}\phi \mapsto \phi(a)$. Si verifica che ζ è un omomorfismo: essendolo già per i gruppi, è sufficiente verificare che $\zeta((a+I)(b+I)) = \zeta(ab+I) = \phi(ab) = \phi(a)\phi(b) = \zeta(a+I)\zeta(b+I)$.

ζ è chiaramente anche un epimorfismo, dal momento che $\forall\, \phi(a) \in \operatorname{Imm}\phi$, $\zeta(a + \operatorname{Ker}\phi) = \phi(a)$. Inoltre, dal momento che $\zeta(a + \operatorname{Ker}\phi) = 0 \iff \phi(a) = 0 \iff a + \operatorname{Ker}\phi = \operatorname{Ker}\phi$, ossia l'identità di $A/\operatorname{Ker}\phi$, si deduce anche che ζ è un monomorfismo. Pertanto ζ è un isomorfismo. □

Corollario 3.1. Sia $\phi : A \to B$ un monomorfismo. $A \cong \operatorname{Imm}\phi$.

Dimostrazione. Poiché ϕ è un monomorfismo, $\operatorname{Ker}\phi = \{0\}$. Allora, per il *Primo teorema di isomorfismo*, $A/\{0\} \cong \operatorname{Imm}\phi$. Dalla *Proposizione 3.1*, si desume che $A \cong A/\{0\}$. Allora, per la proprietà transitiva degli isomorfismi, $A \cong \operatorname{Imm}\phi$. □