Algebra Commutativa

Davide Borra

v. 1.0

davide.borra@studenti.unitn.it - davideborra.github.io

Indice

Sommario
Note del corso di Algebra Commutativa, tenuto dal Prof. E. Ballico nell'A.A. 2024/25, basate sulle note di M. Vergura [Ver] e sul libro di M. Reid [Rei95]

Capitolo 1

Anelli ed ideali

1.1 Generalità

DEF 1.1 (Anello)**.** Un anello commutativo con unità 1 è una quintupla ordinata $(A, +, 0, \cdot, 1)$ in cui $(A, +)$ è un gruppo abeliano, $1 \in A$ e $\cdot : A \times A \to A$ è una mappa di composizione interna detta “prodotto” tale che per ogni $a, b, c \in A$ valgono

- $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ (associatività del prodotto)
- $a \cdot 1 = a$ (esistenza dell'elemento neutro del prodotto)
- $a \cdot (b + c) = a \cdot b + a \cdot c$ (distributività a sinistra)
- $(a + b) \cdot c = a \cdot c + b \cdot c$ (distributività a destra)
- $a \cdot b = b \cdot a$ (commutatività)

Se non è necessario specificare le operazioni, confonderemo l'anello $(A, +, 0, \cdot, 1)$ con il suo supporto A.

Osservazione 1.2.

- $\forall a \in A$, $a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 + a \cdot 0$, quindi $a \cdot 0 = 0$.
- $\forall a, b \in A$, $a(-b) = -ab$, infatti $0 = a \cdot 0 = a(b - b) = ab + a(-b)$.

DEF 1.3 (Sottoanello)**.** A anello; $S \subset A$ si dice sottoanello di A se $1 \in S$, S è un sottogruppo di $(A, +, 0)$ e, per ogni $s, t \in S$, $s \cdot t \in S$.

Esempio 1.1.
Poiché siamo interessati agli anelli con unità, richiediamo che anche i sottoanelli la contengano: ciò non è infatti scontato. Si consideri l'anello dei numeri interi $\mathbb{Z}$, allora i numeri pari $2\mathbb{Z}$ costituiscono un suo sottoanello privo tuttavia dell'unità.

DEF 1.4 (Omomorfismo)**.** A, B anelli, $f : A \to B$ si dice omomorfismo (di anelli) se per ogni $a, b \in A$

- $f(a + b) = f(a) + f(b)$;
- $f(ab) = f(a)f(b)$;
- $f(1) = 1$.

Indichiamo con $\ker f := f^{-1}(\{0\})$ il nucleo dell'omomorfismo.

Osservazione 1.5.

- $f(0) = f(0 + 0) = f(0) + f(0) \implies f(0) = 0$;
- $\forall a \in A, 0 = f(0) = f(a - a) = f(a) + f(-a) \implies f(-a) = -f(a)$;

Esercizio 1.1. *Verificare che un omomorfismo di anelli f è iniettivo* $\iff \ker f = \{0\}$.

Proposizione 1.6. *A, B anelli, $S \subseteq A$ sottoanello, $f : A \to B$ omomorfismo. Allora $f(S) \subseteq B$ è un sottoanello.*

Dimostrazione.

- $f(1) = 1$ per definizione, quindi $1 \in f(S)$;
- Siano $f(a), f(b) \in f(S)$, allora $a, b \in S$, quindi

$$\begin{cases} f(a) + f(b) = f(a+b) \\ a + b \in S \end{cases} \implies f(a) + f(b) \in f(S)$$

$$\begin{cases} f(a)f(b) = f(ab) \\ ab \in S \end{cases} \implies f(a)f(b) \in f(S)$$

QED

DEF 1.7 (Isomorfismo)**.** A, B anelli. Un omomorfismo $f : A \to B$ si dice isomorfismo (di anelli) se esiste un omomorfismo $g : B \to A$ tale che $f \circ g = \mathrm{Id}_B$ e $g \circ f = \mathrm{Id}_A$. In tal caso A e B si dicono isomorfi, e si scrive $A \cong B$.

Esercizio 1.2. *Verificare che $f : A \to B$ è un isomorfismo se e solo se è un omomorfismo biiettivo.*

DEF 1.8 (Ideale)**.** A anello, $I \subset A$ è detto ideale di A se è un sottogruppo di $(A, +, 0)$ e $\forall a \in A, \forall i \in I$, $ai \in I$.

Individuiamo subito degli ideali banali: l'ideale triviale $\{0\}$ e l'ideale improprio A. Un ideale $I \subsetneq A$ si dice **proprio**.

Proposizione 1.9. *A, B anelli, $I \subseteq A$ qualsiasi, $J \subseteq B$ ideale; $f : A \to B$ omomorfismo di anelli. Allora*

1. *Se $1 \in I$, allora I è un ideale se e solo se $I = A$. In particolare f è suriettivo se e solo se $f(A)$ è un ideale.*
2. $\ker f$ *è un ideale di A.*
3. *$f^{-1}(J)$ è un ideale di A.*

Dimostrazione.

1. Siano I un ideale e $a \in A$. Poiché $1 \in I$, $a1 = a \in I$ quindi $I = A$. L'altra implicazione è banale.
2. $0 \in \ker f$ in quanto $f(0) = 0$. Siano $a, b \in \ker f$, $z \in A$ qualsiasi. Allora
   - $0 = f(a) + f(b) = f(a+b) \implies a + b \in \ker f$;
   - $0 = f(a)f(z) = f(az) \implies az \in \ker f$.
3. $0 \in f^{-1}(J)$ in quanto $f(0) = 0$. Siano $a, b \in \ker f$, $z \in A$ qualsiasi. Allora
   - $J \ni f(a) + f(b) = f(a+b) \implies a + b \in f^{-1}(J)$
   - $J \ni f(a)f(z) = f(az) \implies az \in f^{-1}(J)$.

QED

La proposizione precedente ci fa presagire un qualche tipo di collegamento tra ideali ed omomorfismi: in particolare siamo interesati a provare che un $I \subseteq A$ è un ideale se e solo se è il nucleo di un qualche omomorfismo. In questo senso siamo interessati a dimostrare la seguente Proposizione.

Proposizione 1.10. *Sia A un anello e $I \subset A$ un ideale. Allora esistono un anello B e un omomorfismo di anelli $f : A \to B$ tali che f sia suriettiva e* $\ker f = I$.

Per fare questo, costruiamo B come quoziente di A rispetto ad una relazione di equivalenza, che diremo indotta da I. Allora f sarà la mappa di proiezione al quoziente. Osserviamo che se una relazione di equivalenza $\sim \in \mathcal{P}(A^2)$ è compatibile con le operazioni, *i.e.*

$$a \sim c, b \sim d \implies \begin{cases} a+b \sim c+d \\ ab \sim cd \end{cases}$$

allora $[0]_\sim = \{x \in A \mid x \sim 0\}$ è un ideale di A. Risulta tuttavia più interessante il fatto che anche un procedimento inverso sia lecito: dato un ideale, è possibile costruire una relazione di equivalenza $\sim_I$ che sia compatibile con le operazioni e tale che $[0]_{\sim_I} = I$. Definiamo quindi $\sim_I \in \mathcal{P}(A^2)$ come

$$a \sim_I b \iff a - b \in I \qquad \forall a, b \in A.$$

La verifica degli assiomi di relazione di equivalenza è immediata, così come la compatibilità con le operazioni. Indichiamo inoltre

$$[a]_I = \{b \in A \mid b \sim a\} = \{b \in A \mid a - b \in I\} = \{a + i \mid i \in I\} =: a + I.$$

Per ottenere il risultato desiderato è quindi sufficiente definire una struttura di anello su $A/I := A/\sim_I = \{a + I \mid a \in A\}$ ponendo

$$(a+I) + (b+I) := (a+b) + I \qquad \text{e} \qquad (a+I)(b+I) := (ab) + I.$$

Un'immediata verifica permette di dedurre che, con questa struttura, A/I è a sua volta un anello commutativo con unità $1 + I$, e che la mappa $f : A \twoheadrightarrow A/I$ data da $f(a) = a + I$ soddisfa le condizioni desiderate. Da questa costruzione segue inoltre direttamente il Primo Teorema di Isomorfismo.

Teorema 1.11 (Isomorfismo I)**.** *A, B anelli, $f : A \to B$ omomorfismo. Allora esiste un unico isomorfismo $\varphi : A/\ker f \to f(A)$ tale per cui il seguente diagramma commuti*

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[d, two heads, "\pi"'] & B \\ A/\ker f \arrow[r, dashed, "\sim", "\exists! \varphi"'] & f(A) \arrow[u, hook, "\iota"'] \end{tikzcd}$$

dove $\pi : A \twoheadrightarrow A/\ker f$ è la proiezione al quoziente mentre $\iota : f(A) \hookrightarrow B$ è l'inclusione canonica.

Dimostrazione. La dimostrazione è analoga a quella di ogni altro primo teorema di isomorfismo, pertanto si assume che il lettore ne sia già a conoscenza. QED

Proposizione 1.12. *A anello, $I \subseteq A$ ideale. Vi è una corrispondenza biunivoca tra gli ideali di A contenenti I e gli ideali di A/I. Se $\pi : A \twoheadrightarrow A/I$ è l'omomorfismo di passaggio al quoziente, tale biiezione è data associando ad un ideale J di A la sua immagine $\pi(J)$ mediante π.*

Dimostrazione. Inizialmente osserviamo che, poiché π è suriettiva per costruzione, manda ideali di A in ideali di A/I. Infatti, preso un ideale $K \subseteq A$, banalmente $\pi(K)$ è un sottogruppo di A/I. Dati quindi $a \in K$ e $\alpha \in A/I$ ($\implies$ esiste un $b \in A$ tale che $\pi(b) = \alpha$) allora $\alpha\pi(a) = \pi(b)\pi(a) = \pi(ba) \in \pi(K)$.

Mostriamo ora che la mappa $I \mapsto \pi(I)$ è biiettiva:

$\boxed{\twoheadrightarrow}$ Sia $J \subset A/I$ ideale. Allora $\pi^{-1}(J)$ è un ideale per Proposizione 1.9 e contiene I in quanto $0 + I \in J$. Inoltre, poiché π è suriettiva, $\pi(\pi^{-1}(J)) = J$.

$\boxed{\hookrightarrow}$ Siano $I_1, I_2 \subseteq A$ ideali con $I \subset I_1$, $I \subset I_2$ e tali che $\pi(I_1) = \pi(I_2)$. Proviamo che $I_1 = I_2$:

- $\boxed{\subseteq}$ Sia $a \in I_1$, allora $\pi(a) \in \pi(I_1) = \pi(I_2)$. Deve quindi esistere un $b \in I_2$ tale che $\pi(b) = \pi(a)$, ovvero $\pi(b - a) = 0$, da cui $b - a = i \in \ker \pi = I$. Segue quindi che $a = b + i \in I_2$.
- $\boxed{\supseteq}$ Analogo. QED

Proposizione 1.13. *Siano A, B, C anelli, $h : A \twoheadrightarrow B$ un omomorfismo suriettivo e $\gamma : A \to C$ un omomorfismo. Allora le seguenti condizioni sono equivalenti*

(1) Esiste un omomorfismo $g : B \to C$ tale per cui il seguente diagramma commuti

$$\begin{tikzcd} A \arrow[r, two heads, "h"] \arrow[dr, "\gamma"'] & B \arrow[d, dashed, "\exists g"] \\ & C \end{tikzcd}$$

(2) Per ogni $a, a' \in A$, $h(a) = h(a') \implies \gamma(a) = \gamma(a')$

Inoltre tale omomorfismo è unico.

Dimostrazione.

$\boxed{!}$ L'unicità è banale: siano $f, g : B \to C$ tali per cui il diagramma commuti. Allora per ogni $b \in B$ deve esistere un $a \in A$ tale che $h(a) = b$ (h è suriettiva), quindi

$$g(b) = g(h(a)) = \gamma(a) = f(h(a)) = f(b).$$

$\boxed{\Rightarrow}$ Supponiamo che un tale omomorfismo esista e siano $a, a' \in A$ tali che $h(a) = h(a')$. Allora

$$\gamma(a) = g(h(a)) = g(h(a')) = \gamma(a').$$

$\boxed{\Leftarrow}$ Supponiamo che valga la (2), allora possiamo definire $g : B \to C$ come segue: per ogni $b \in B$, sia $a \in h^{-1}(b)$, allora poniamo $g(b) := \gamma(a)$. Questa è una buona definizione per (2) e un omomorfismo in quanto h e γ lo sono.

QED

Osservazione 1.14. (2) è equivalente a richiedere che $\ker h \subseteq \ker \gamma$.

1.2 Operazioni tra ideali

1.2.1 Intersezione e generazione

Proposizione 1.15. *Data una famiglia $\{I_\alpha\}_{\alpha\in\Gamma}$ di ideali in A ($\Gamma \neq \varnothing$), allora l'intersezione*

$$I := \bigcap_{\alpha\in\Gamma} I_\alpha$$

è un ideale in A.

Dimostrazione. Verifichiamo gli assiomi di ideale:

- $0 \in I_\alpha \forall\alpha \implies 0 \in I$;
- $x, y \in I \implies x, y \in I_\alpha \forall\alpha \implies x + y \in I_\alpha \forall\alpha \implies x + y \in I$;
- Fissato $k \in A$, $x \in I \implies x \in I_\alpha \forall\alpha \implies kx \in I_\alpha \forall\alpha \implies kx \in I$.

QED

DEF 1.16 (Generazione)**.** A anello, $S \subseteq A$ qualsiasi. Si dice "ideale generato da S" il più piccolo ideale $\langle S\rangle$ contenente S.

Osservazione 1.17.

- Per il Lemma del Minimo vale l'uguaglianza
$$\langle S\rangle = \bigcap\{I \subset A \mid I \text{ ideale}; I \supseteq S\}$$
- Tale ideale esiste sempre in quanto A stesso è un ideale contenente S.
- Se S è un insieme finito di elementi, diciamo $S = \{a_1, \ldots, a_k\}$, allora vale
$$\langle S\rangle = \left\{\sum_{i=1}^{k} c_i a_i \mid c_i \in A; a_i \in S\right\}$$

in quanto il membro a destra è un ideale contenente S ed è contenuto in ogni ideale contenente S.

- Se $S = \varnothing$, allora $\langle S \rangle = \{0\}$.

DEF 1.18 (Generatori)**.** Sia A un anello, dichiamo che un ideale $I \subseteq A$ è finitamente generato se esistono $\{g_1, \dots, g_n\} \subset I$ tali che $I = \langle \{g_1, \dots, g_n\} \rangle := \langle g_1, \dots, g_n \rangle$. Più in generale, gli elementi di un $S \subset I$ tale che $I = \langle S \rangle$ si dicono generatori di I.

Osservazione 1.19. Ogni ideale possiede un sistema di generatori: l'ideale stesso.

DEF 1.20. Un ideale I si dice principale se esiste un $a \in A$ tale che $I = \langle a \rangle$. Se un anello A è tale che *ogni* suo ideale è principale, si dice essere *a ideali principali*.

DEF 1.21 (Invertibili)**.** Sia A un anello con $A \neq \{0\}$. Un elemento $a \in A$ ssi dice invertibile se esiste un $b \in A$ tale che $ab = ba = 1$. Indichiamo con $A^\times$ l'insieme degli elementi invertibili di A.

Osservazione 1.22.

- $A^\times \neq \varnothing$ in quanto $1 \in A^\times$;
- $a \in A$ invertibile $\implies a \neq 0$;
- l'inverso, se esiste, è unico;
- a, b invertibili $\implies a^{-1}, b^{-1}, ab$ invertibili, quindi $A^\times$ è un sottogruppo abeliano del monoide commutativo $(A, \times, 1)$.
- Se $A \neq \{0\}$, $I \subset A$ è l'ideale improprio se e solo se contiene un elemento invertibile.

DEF 1.23 (Campo)**.** Sia A un anello commutativo con unità $1 \neq 0$. Allora A si dice campo se ogni elemento non zero è invertibile.

Proposizione 1.24. *Sia A un anello non banale, allora A è un campo se e solo se i suoi unici ideali sono $\{0\}$ e A.*

Dimostrazione.

$\boxed{\Rightarrow}$ Siano $\{0\} \neq I \subset A$ e $0 \neq a \in I$, allora $1 = aa^{-1} \in I$, da cui $I = A$.

$\boxed{\Leftarrow}$ Sia $a \in A^*$, allora $a \in \langle a \rangle \neq \{0\}$, quindi $\langle a \rangle = A$, per cui $1 \in \langle a \rangle$. Deve pertanto esistere un $x \in \langle a \rangle$ tale che $ax = xa = 1$. QED

1.2.2 Somma

DEF 1.25 (Somma)**.** A anello, I, J ideali in A. Allora la somma di I e J è l'insieme

$$I + J := \{i + j \mid i \in I, j \in J\}.$$

Proposizione 1.26. *$I + J$ è un ideale e vale $I + J = \langle I \cup J \rangle$*

Dimostrazione. Facile. $\curvearrowright$ QED

Procedendo induttivamente possiamo definire la somma di una famiglia finita di ideali.

Osservazione 1.27. $I_1, I_2, J \subset A$ ideali, allora

$$(J \cap I_1) + (J \cap I_2) \subseteq J \cap (I_1 + I_2).$$

Bibliografia

[Gra] Willem Adriaan de Graaf. *Algebra*. Trento. URL: https://degraaf.maths.unitn.it/algnotes/algebranotes.pdf.

[Occ] Gianluca Occhetta. *Introduzione alla Geometria Algebrica*. Trento. URL: https://sites.google.com/unitn.it/occhetta/home/note-di-corsi?authuser=0#h.7y00c9kbd8e5.

[Rei95] Miles Reid. *Undergraduate Commutative Algebra*. London Mathematical Society Student Texts. Cambridge University Press, 1995.

[Sta24] Mima Stanojkovski. *Note per il corso di Teoria dei Gruppi*. 2024.

[Ver] Marco Vergura. *Dispense per il corso di Algebra Commutativa*.