Lezione 5

Prerequisiti: Lezione 2, Lezione 3.

Gli anelli

In questa lezione diamo il secondo esempio di struttura algebrica astratta, che si aggiunge a quella di gruppo, definita nella Lezione 2. Questa nuova struttura, detta *anello*, include quella di gruppo, ed è costituita da un insieme dotato di due operazioni. Storicamente, il concetto di anello ha origine dagli studi compiuti dai matematici tedeschi Richard Dedekind (1831-1916) e Ernst Eduard Kummer (1810-1893) intorno a particolari sottoinsiemi del campo complesso.

Definizione 5.1 Si dice *anello* ogni terna ordinata $(A,+,\cdot)$, ove A è un insieme non vuoto, e $+,\cdot$ sono operazioni su A verificanti le seguenti condizioni:

(a) $(A,+)$ è un gruppo abeliano;
(b) per ogni $a,b,c \in A$, $a\cdot(b\cdot c)=(a\cdot b)\cdot c$ ($\cdot$ è associativa);
(c) per ogni $a,b,c \in A$, $a\cdot(b+c)=a\cdot b+a\cdot c$, $(b+c)\cdot a=b\cdot a+c\cdot a$ ($\cdot$ è *distributiva* rispetto a +).

L'operazione $\cdot$ si dice *prodotto* o moltiplicazione; l'operazione + si dice *somma* o *addizione*.
Il gruppo $(A,+)$ è detto *gruppo additivo* dell'anello A. Il suo elemento neutro viene denotato 0_A (o, più semplicemente, 0) ed è detto *zero* (talvolta anche *elemento nullo*).

L'anello si dice *commutativo* se il prodotto è commutativo.

L'anello si dice *unitario* se esiste un elemento neutro del prodotto. In tal caso questo viene denotato 1_A (o, più semplicemente, 1) ed è detto *uno*.

Nota Nel seguito, ove non sia necessario precisare le operazioni, scriveremo semplicemente A al posto di $(A,+,\cdot)$. Salvo avviso contrario, la somma sarà sempre indicata con + ed il prodotto con $\cdot$.
Per semplicità, spesso il simbolo $\cdot$ si omette e si scrive ab al posto di $a\cdot b$.
Scriveremo anche $a-b$ al posto di $a+(-b)$.

Proposizione 5.2 *(Proprietà dello zero, degli opposti in un anello. Unicità dell'uno.)* Sia A un anello.

(a) Per ogni $a \in A$, $a0=0a=0$.
(b) Per ogni $a,b \in A$, $(-a)b=a(-b)=-ab$, $(-a)(-b)=ab$.
(c) Se l'anello A è unitario, allora l'elemento uno è unico.

Dimostrazione: (a) Per ogni $a \in A$,

$$a0=a(0+0)=a0+a0,$$

ove la prima uguaglianza segue dal fatto che 0 è idempotente rispetto alla somma (vedi Esercizio 2.10) e la seconda dalla proprietà distributiva. Segue che $a0$ è un elemento idempotente del gruppo additivo di A, e quindi, per l'Esercizio 2.10, coincide con l'elemento neutro, ossia $a0 = 0$. In maniera analoga si prova che $0a = 0$.

(b) Per ogni $a, b \in A$,

$$(-a)b + ab = (-a + a)b = 0b = 0,$$

dove abbiamo usato la proprietà distributiva e la parte (a) della Proposizione. Ciò prova che $(-a)b$ è l'opposto di ab nel gruppo $(A, +)$. Analogamente si prova che $a(-b)$ è l'opposto di ab.
Da quest'ultima affermazione (valida per arbitrari elementi dell'anello) segue, in particolare, che, per ogni $a, b \in A$, $(-a)(-b)$ è l'opposto di $(-a)b$. Ma l'elemento $(-a)b$, come abbiamo appena visto, ha come opposto ab. Quindi, per l'unicità dell'opposto (v. Proposizione 2.7 (b)), $(-a)(-b) = ab$.
(c) Siano $1, 1'$ elementi neutri del prodotto dell'anello unitario A. Allora $1 = 11' = 1'$. □

Esempio 5.3 (a) Sono anelli commutativi unitari gli insiemi $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ rispetto alle usuali operazioni di somma e prodotto.
(b) Sia $X = \{x\}$. L'insieme X può essere dotato di una struttura di anello (commutativo e unitario) scegliendo come somma e come prodotto l'unica operazione binaria definita su X, ossia ponendo $x + x = x$, $x \cdot x = x$. L'anello così ottenuto si dice *anello banale* (o *anello nullo*). L'unico suo elemento è, contemporaneamente, elemento zero ed elemento uno. Viceversa, un anello A in cui $0 = 1$ è necessariamente banale. Infatti, per ogni $a \in A$, si ha, in base alla Proposizione 5.2 (a), $a = a1 = a0 = 0$. Quindi 0 è l'unico elemento dell'anello A.

Diamo, di seguito, alcune definizioni e proprietà che individuano particolari elementi di un anello.

Definizione 5.4 Sia A un anello unitario. Un elemento a di A si dice *invertibile a destra* se esiste $u \in A$ tale che $au = 1$. In tal caso u si dice un *inverso destro* di A. Un elemento a di A si dice *invertibile a sinistra* se esiste $v \in A$ tale che $va = 1$. In tal caso v si dice un *inverso sinistro* di A.
Un elemento a di A si dice *invertibile* se esiste $w \in A$ tale che $aw = wa = 1$. In tal caso w si dice *inverso* di a.

Nota Gli elementi invertibili di un anello unitario si chiamano talvolta anche *unità*.

Proposizione 5.5 *(Invertibilità)* In un anello unitario, un elemento è invertibile se e solo se è invertibile sia a destra sia a sinistra. In tal caso l'inverso è unico, ed è l'unico inverso destro e l'unico inverso sinistro.

Dimostrazione: Sia A un anello unitario e sia $a \in A$. Se a è invertibile, allora, se w è inverso di a, w è anche inverso destro e sinistro di A, quindi a è invertibile a destra e a sinistra. Viceversa, supponiamo che a verifichi quest'ultima condizione, e siano u un suo inverso destro e v un suo inverso sinistro. Allora si ha

$$u = 1 \cdot u = (va)u = v(au) = v \cdot 1 = v.$$

Ciò prova che $u = v$ è l'unico inverso destro e l'unico inverso sinistro di *a*, e quindi è l'unico inverso di *a*. □

Nota Data l'unicità dell'inverso, per ogni elemento invertibile *a* di un anello unitario, possiamo denotare l'inverso di *a* con a^{-1}.

Osservazione 5.6 In un anello commutativo unitario le nozioni di invertibilità a sinistra, invertibilità a destra ed invertibilità coincidono, così come quelle di inverso sinistro, inverso destro ed inverso. Ciò non è necessariamente vero in un anello unitario non commutativo.

Esempio 5.7 Nell'anello $\mathbb{Z}$ gli unici elementi invertibili sono 1 e –1, che sono ognuno inverso di se stesso. Negli anelli $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ sono invertibili tutti gli elementi diversi da zero. Per il campo complesso si veda, in particolare, la proprietà (f) della Lezione 1.
Osserviamo che in un anello non nullo lo zero non è mai invertibile: infatti, per ogni elemento *a* dell'anello si ha che $a0 = 0 \neq 1$, e quindi nessun elemento *a* è inverso di 0.

Proposizione 5.8 *(Gruppo delle unità)* L'insieme degli elementi invertibili di un anello unitario, munito della restrizione del prodotto dell'anello, è un gruppo moltiplicativo.

Dimostrazione: Sia *A* un anello unitario, e sia *U* l'insieme dei suoi elementi invertibili. Allora *U* è chiuso rispetto al prodotto di *A*: infatti, per ogni $a, b \in U$, si ha che $b^{-1}a^{-1}$ è l'inverso di *ab* (lo si dimostra come la Proposizione 2.8 (b)), e quindi $ab \in U$. Quindi il prodotto di *A* induce per restrizione un prodotto su *U*. Proviamo ora che, rispetto a tale operazione, *U* è un gruppo. La proprietà associativa è banalmente verificata, essendo vera per il prodotto di *A*. L'elemento neutro è 1 (che appartiene ad *U*, in quanto evidentemente invertibile). L'esistenza degli inversi è assicurata dalla stessa definizione di *U*. □

Definizione 5.9 L'insieme degli elementi invertibili dell'anello *A* di dice *gruppo delle unità* di *A*, ed è denotato $\mathscr{U}(A)$.

Esempio 5.10 In base a quanto visto nell'Esempio 5.7, $\mathscr{U}(\mathbb{Z}) = \{1, -1\} = R_2$, $\mathscr{U}(\mathbb{Q}) = \mathbb{Q}^*$, $\mathscr{U}(\mathbb{R}) = \mathbb{R}^*$, $\mathscr{U}(\mathbb{C}) = \mathbb{C}^*$.

Definizione 5.11 Un anello unitario, non ridotto a un solo elemento, in cui ogni elemento non nullo è invertibile si dice un *corpo*. Un corpo commutativo si dice un *campo*.

In altri termini, un anello (commutativo) unitario *A* è un corpo (un campo) se $\mathscr{U}(A) = A \setminus \{0\}$. Indicheremo $A \setminus \{0\}$ con A^*. In tal caso, $\mathscr{U}(A)$ si dice anche il *gruppo moltiplicativo* del corpo (campo) *A*.

Esempio 5.12 L'anello $\mathbb{Z}$ non è un campo. Gli anelli $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ sono campi.

Definizione 5.13 Sia *A* un anello e sia $a \in A$, $a \neq 0$. Allora a si dice un *divisore dello zero* se esiste $b \in A$, $b \neq 0$ tale che $ab = 0$ oppure $ba = 0$. Altrimenti *a* si dice un elemento *regolare*.

Nota Alcuni autori includono lo zero tra i divisori dello zero. Ciò è lecito in base alla Proposizione 5.2 (a).

Definizione 5.14 Un anello si dice *integro* se è privo di divisori dello zero (equivalentemente, se ogni elemento diverso dallo zero è regolare).
Un anello commutativo unitario integro (non banale) si dice un *dominio d'integrità*.

Osservazione 5.15 Un anello A è integro se e solo se in esso vale la *legge di annullamento del prodotto*, ossia, per ogni $a,b \in A$, $ab = 0 \Rightarrow a = 0$ oppure $b = 0$.
Un divisore dello zero è un elemento che viola la legge di annullamento del prodotto.

Esempio 5.16 Gli anelli $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ sono domini d'integrità.

Più avanti conosceremo molti esempi di anelli non integri.

Proposizione 5.17 In un anello unitario non nullo, ogni elemento invertibile è regolare.

Dimostrazione: Sia A un anello unitario non nullo e sia $a \in A$ un elemento invertibile. Allora, per quanto osservato nell'Esempio 5.7, $a \neq 0$. Sia $b \in A$ tale che $ab = 0$ oppure $ba = 0$. Nel primo caso $0 = a^{-1}0 = a^{-1}(ab) = (a^{-1}a)b = 1b = b.$ Nella prima e nella terza uguaglianza sono state applicate, rispettivamente, la Proposizione 5.2 (a) e la proprietà associativa del prodotto. In maniera analoga si prova che da $ba = 0$ segue $b = 0$. Ciò dimostra che non esiste, per a, un elemento b verificante la condizione della Definizione 5.13. Quindi a è regolare. □

Corollario 5.18 Ogni corpo è integro. Ogni campo è un dominio d'integrità.

Dimostrazione: In un corpo ogni elemento non nullo è invertibile, quindi, in base alla Proposizione 5.17, ogni elemento non nullo è regolare. □

Osservazione 5.19 L'anello $\mathbb{Z}$ è un dominio d'integrità che non è un campo. Quindi non vale il viceversa del Corollario 5.18.

Definizione 5.20 Sia A un anello e sia $a \in A$. Allora a si dice *cancellabile a destra* se, per ogni $x, y \in A$, $xa = ya \Rightarrow x = y.$ Si dice *cancellabile a sinistra* se, per ogni $x, y \in A$, $ax = ay \Rightarrow x = y$. Si dice *cancellabile* se è cancellabile a destra e a sinistra.

Proposizione 5.21 In un anello, un elemento non nullo è regolare se e solo se è cancellabile.

Dimostrazione: Sia A un anello. Sia $a \in A, a \neq 0$. Supponiamo che a sia regolare. Siano $x, y \in A$ tali che $xa = ya$. Allora, per la proprietà distributiva e la Proposizione 5.2 (b):

$$0 = xa - ya = xa + (-ya) = xa + (-y)a = (x - y)a.$$

Essendo a regolare, segue che $x - y = 0,$ ossia $x = y$. Ciò prova che a è cancellabile a destra. Analogamente si prova che a è cancellabile a sinistra. Viceversa, supponiamo che a sia cancellabile. Sia $b \in A$ tale che $ab = 0$ oppure $ba = 0$. Nel primo caso, in base alla Proposizione 5.2 (a), si ha $ab = a0$. Essendo a cancellabile a sinistra, segue che $b = 0$. Analogamente si deduce che anche nel secondo caso $b = 0$. Ciò prova che a è regolare. □

Passiamo ora a considerare le sottostrutture di un anello. La prossima definizione è analoga a quella di sottogruppo (Definizione 2.16), ma tiene conto del fatto che, in un anello, le operazioni da considerare sono due.

Definizione 5.22 Sia $(A,+,\cdot)$ un anello, e sia B un sottoinsieme non vuoto di A. Allora B si dice un *sottoanello* di A se

(a) B è chiuso rispetto alle operazioni $+$ e $\cdot$;
(b) B è un anello rispetto alle operazioni $+$ e $\cdot$ ristrette.

Esempio 5.23 (a) Ogni anello è sottoanello di se stesso (*sottoanello totale).* Dato un anello A, il suo sottoinsieme ridotto al solo zero è un sottoanello di A, detto *sottoanello banale* o *nullo*: alla luce dell'Esempio 5.3 (b), basta osservare che $0+0=0, 0\cdot 0=0$.
(b) $\mathbb{Z}$ è un sottoanello di $\mathbb{Q}$, che è un sottoanello di $\mathbb{R}$, che è un sottoanello di $\mathbb{C}$.

Come i sottogruppi, anche i sottoanelli si possono caratterizzare attraverso proprietà diverse (e più agevoli da verificare) rispetto a quelle contenute nella definizione.

Proposizione 5.24 (*Prima caratterizzazione dei sottoanelli*) Sia A un anello, e sia B un sottoinsieme non vuoto di A. Allora B è un sottoanello di A se e solo se

(i) B è un sottogruppo del gruppo additivo di A;
(ii) B è chiuso rispetto al prodotto di A.

Dimostrazione: Proviamo che B soddisfa le condizioni (a) e (b) della Definizione 5.22 se e solo se soddisfa le condizioni (i) e (ii). Supponiamo che (i) e (ii) siano verificate. Allora B è chiuso rispetto alla somma di A in virtù della (i). Inoltre, in base alla (ii), è chiuso rispetto al prodotto. Dunque B soddisfa la condizione (a) della Definizione 5.22. Ora il gruppo additivo di A, per definizione, è abeliano. In virtù del Corollario 2.26, segue che B, dotato della somma ristretta, è anch'esso un gruppo abeliano. Inoltre il prodotto ristretto a B è associativo e distributivo rispetto alla somma ristretta a B (poiché queste proprietà valgono per il prodotto e la somma di A). Ciò prova che B è un anello rispetto alle operazioni ristrette, ossia B verifica la condizione (b) della Definizione 5.22.
Viceversa, supponiamo che B verifichi le condizioni (a) e (b) della Definizione 5.22. Allora, in virtù della (a), B è chiuso rispetto alla somma di A, e, in virtù della (b), è un gruppo rispetto alla somma ristretta. Per definizione di sottogruppo (Definizione 2.16), ciò significa che vale la (i). D'altra parte dalla (a) segue immediatamente la (ii). □

Questa caratterizzazione ne produce un'altra, più semplice.

Corollario 5.25 (*Seconda caratterizzazione dei sottoanelli*) Sia A un anello, e sia B un sottoinsieme non vuoto di A. Allora B è un sottoanello di A se e solo se

(I) per ogni $a,b\in B$, $a-b\in B$;
(II) B *è* chiuso rispetto al prodotto di A.

Dimostrazione: In base alla caratterizzazione dei sottogruppi (Proposizione 2.24), per B la condizione (i) della Proposizione 5.24 è equivalente alla (I), mentre la (ii) della Proposizione 5.24 è identica alla (II). Quindi B verifica le condizioni di questo corollario se e solo se verifica le condizioni della proposizione precedente, il che, in base alla stessa proposizione, avviene se e solo se B è un sottoanello di A. □

Esercizio 5.26 Provare che, per ogni numero naturale n, l'insieme dei multipli di n è un sottoanello di $\mathbb{Z}$.

Svolgimento: Avevamo già provato, nell'Esercizio 2.27 (a), che questo insieme, allora denotato H_n, è un sottogruppo del gruppo $(\mathbb{Z},+)$. In base alla prima caratterizzazione di sottoanello, resta da provare che H_n è chiuso rispetto al prodotto: per ogni $a,b\in\mathbb{Z}$, si ha $(na)(nb)=n(anb)\in H_n$.

Osservazione 5.27 Per ogni numero naturale $n\geq 2$, l'anello H_n non è unitario. Infatti, per ogni $a\in\mathbb{Z}$, na non è elemento neutro del prodotto di H_n: basta osservare che $(na)n\neq n$. Sono invece unitari $H_0=\{0\}$ e $H_1=\mathbb{Z}$.

Il prossimo enunciato si prova come il Corollario 2.26.

Proposizione 5.28 Ogni sottoanello di un anello commutativo è commutativo.

Osservazione 5.29 Non vale l'analogo della Proposizione 5.28 per gli anelli unitari: un sottoanello di un anello unitario non è necessariamente unitario, come abbiamo visto nell'Esempio 5.26. Inoltre, se un sottoanello di un anello unitario è unitario, non ha necessariamente lo stesso elemento uno: il sottoanello nullo di un anello unitario non nullo ha 0 come elemento neutro del prodotto, ove, in base all'Esempio 5.3 (b), $0\neq 1$.

Proposizione 5.30 Sia A un anello unitario. Se B è un sottoanello di A tale che $1\in B$, allora $\mathscr{U}(B)$ è un sottogruppo di $\mathscr{U}(A)$.

Dimostrazione: Osserviamo preliminarmente che $\mathscr{U}(B)\subset\mathscr{U}(A)$: infatti ogni elemento invertibile in B è invertibile anche in A, dove ha lo stesso inverso. Inoltre si ha che $1\in\mathscr{U}(B)$, quindi $\mathscr{U}(B)\neq\varnothing$. In base alla Proposizione 5.8, $\mathscr{U}(B)$ è un gruppo rispetto al prodotto di B: ma questo è la restrizione del prodotto di A (e quindi anche la restrizione del prodotto di $\mathscr{U}(A)$). Quindi, in base alla definizione di sottogruppo, $\mathscr{U}(B)$ è un sottogruppo di $\mathscr{U}(A)$. □

Esempio 5.31 Il gruppo $\mathscr{U}(\mathbb{Z})=\{-1,1\}$ è un sottogruppo di $\mathscr{U}(\mathbb{Q})=\mathbb{Q}^*$, che è un sottogruppo di $\mathscr{U}(\mathbb{R})=\mathbb{R}^*$, che è un sottogruppo di $\mathscr{U}(\mathbb{C})=\mathbb{C}^*$.

Definizione 5.32 Sia $(K,+,\cdot)$ un corpo (campo), e sia L un sottoinsieme non vuoto di K. Allora L si dice un *sottocorpo (sottocampo)* di K se

(a) L è chiuso rispetto alle operazioni $+$ e $\cdot$;
(b) L è un corpo (campo) rispetto alle operazioni $+$ e $\cdot$ ristrette.

Corollario 5.33 Sia K un corpo (campo), e sia L un suo sottocorpo (sottocampo). Allora

(a) L è un sottoanello di K;
(b) L^* è un sottogruppo di K^*.

Dimostrazione: (a) è conseguenza delle Definizioni 5.22 e 5.32. L'enunciato (b) discende dalla Definizione 5.11 e dalla Proposizione 5.30. □

Diamo ora una nozione che corrisponde, nell'ambito degli anelli, a quella introdotta per i gruppi nella Lezione 3.

Definizione 5.34 Siano $(A_1,+_1,\cdot_1)$ e $(A_2,+_2,\cdot_2)$ anelli. Un'applicazione $f: A_1 \to A_2$ si dice un *omomorfismo (di anelli)* se, per ogni $a,b \in A_1$,

$$f(a +_1 b) = f(a) +_2 f(b); \quad (1)$$
$$f(a \cdot_1 b) = f(a) \cdot_2 f(b). \quad (2)$$

Se $(A_1,+_1,\cdot_1) = (A_2,+_2,\cdot_2)$, f si dice *endomorfismo.* Un omomorfismo bigettivo si dice *isomorfismo*. Un endomorfismo bigettivo si dice *automorfismo*. Inoltre, un omomorfismo iniettivo si dice *monomorfismo*, ed un omomorfismo suriettivo si dice *epimorfismo.*

In altri termini, un omomorfismo è un'applicazione tra anelli che rispetta entrambe le operazioni di anello, sia la somma, sia il prodotto.

Esempio 5.35 (a) Sia $(A,+,\cdot)$ un anello. Se B è un sottoanello di A, l'applicazione di inclusione insiemistica $i: B \to A$ è un monomorfismo di anelli. In particolare, l'applicazione identica id_A di A è un automorfismo dell'anello A.
(b) Siano $(A_1,+_1,\cdot_1)$ e $(A_2,+_2,\cdot_2)$ anelli, e sia 0_2 l'elemento zero di A_2. Allora l'applicazione costante $f: A_1 \to A_2$ definita da $f(a) = 0_2$ per ogni $a \in A_1$ è un omomorfismo di anelli. Infatti, per ogni $a,b \in A_1$,

$$f(a +_1 b) = 0_2 = 0_2 +_2 0_2 = f(a) +_2 f(b);$$
$$f(a \cdot_1 b) = 0_2 = 0_2 \cdot_2 0_2 = f(a) \cdot_2 f(b).$$

Questo omomorfismo si dice *omomorfismo banale* o *nullo.*

Osservazione 5.36 Dalla condizione (1) della Definizione 5.34 si evince che ogni omomorfismo di anelli è un omomorfismo di gruppi tra i gruppi additivi degli stessi anelli. Questa constatazione è utile alle dimostrazioni dei prossimi enunciati.

Proposizione 5.37* *(Proprietà di conservazione degli omomorfismi di anelli)* Siano $(A_1,+_1,\cdot_1)$ e $(A_2,+_2,\cdot_2)$ anelli e sia $f: A_1 \to A_2$ un omomorfismo di anelli. Allora valgono le seguenti proprietà.

(a) Se B_1 è un sottoanello di A_1, allora $f(B_1)$ è un sottoanello di A_2.
(b) Se B_2 è un sottoanello di A_2, allora $f^{-1}(B_2)$ è un sottoanello di A_1.

Dimostrazione: Proviamo solo (a). In base alla Proposizione 3.3 (c), $f(B_1)$ è un sottogruppo del gruppo additivo di A_2. Inoltre è chiuso rispetto al prodotto: infatti, per ogni $a,b \in B_1$, $a \cdot_1 b \in B_1$ (poiché B_1 è un sottoanello di A_1), e quindi $f(a) \cdot_2 f(b) = f(a \cdot_1 b) \in f(B_1)$. La tesi segue allora dalla prima caratterizzazione dei sottoanelli. La dimostrazione di (b) è lasciata per esercizio. □

Esercizio 5.38 Sia $n \in \mathbb{N}$ e sia $f_n: \mathbb{Z} \to \mathbb{Z}$ l'applicazione definita da $a \mapsto na$ per ogni $a \in \mathbb{Z}$. Dire se f_n è un omomorfismo di anelli.

Svolgimento: Abbiamo già provato, nell'Esempio 3.9, che f_n è un omomorfismo di gruppi, ossia soddisfa la condizione (1) della Definizione 5.34. Resta da verificare se soddisfa la condizione (2).

Si ha, per ogni $a,b\in\mathbb{Z}$, $f_n(ab)=nab$, mentre $f_n(a)\,f_n(b)=nanb$. Dunque $f_0(ab)=f_0(a)\,f_0(b)=0$, e $f_1(ab)=f_1(a)\,f_1(b)=ab$, per cui la condizione (2) è soddisfatta quando $n=0$ oppure $n=1$. Non è soddisfatta, invece, quando $n\geq 2$. In tal caso, infatti, essa è violata, ad esempio, per $a=b=1$, poiché $f_n(1\cdot 1)=n$, mentre $f_n(1)\,f_n(1)=n^2$. In conclusione, f_n è un omomorfismo di anelli se e solo se $n\in\{0,1\}$: f_0 è l'endomorfismo nullo di $\mathbb{Z}$, f_1 è l'automorfismo identico di $\mathbb{Z}$.

Definizione 5.39 Siano $(A_1,+_1,\cdot_1)$ e $(A_2,+_2,\cdot_2)$ anelli e sia $f:A_1\to A_2$ un omomorfismo di anelli. Allora si dice *nucleo* di f l'insieme

$$\operatorname{Ker} f = f^{-1}\left(\{0_2\}\right)=\left\{a\in A_1 \middle| f(a)=0_2\right\},$$

ove 0_2 è l'elemento zero di A_2.
Si dice *immagine* di f l'insieme

$$\operatorname{Im} f = f\left(A_1\right)=\left\{f(a)\middle| a\in A_1\right\}.$$

In altri termini, il nucleo e l'immagine di un omomorfismo di anelli f sono il nucleo e l'immagine di f come omomorfismo di gruppi.

Dalla Proposizione 5.37 segue immediatamente il prossimo enunciato.

Corollario 5.40 Siano $(A_1,+_1,\cdot_1)$ e $(A_2,+_2,\cdot_2)$ anelli e sia $f:A_1\to A_2$ un omomorfismo di anelli. Allora $\operatorname{Ker} f$ è un sottoanello di A_1 ed $\operatorname{Im} f$ è un sottoanello di A_2.

Il seguente risultato è una semplice trascrizione della Proposizione 3.8:

Proposizione 5.41 *(Caratterizzazione di monomorfismi ed epimorfismi di anelli)* Siano $(A_1,+_1,\cdot_1)$ e $(A_2,+_2,\cdot_2)$ anelli e sia $f:A_1\to A_2$ un omomorfismo di anelli. Allora

(a) f è un monomorfismo se e solo se il nucleo di f è il sottoanello banale di A_1;
(b) f è un epimorfismo se e solo se l'immagine di f è il sottoanello totale di A_2.

Proposizione 5.42* *(Epimorfismi di anelli ed elementi uno)* Siano $(A_1,+_1,\cdot_1)$ e $(A_2,+_2,\cdot_2)$ anelli e sia $f:A_1\to A_2$ un epimorfismo di anelli. Allora, se A_1 è unitario, anche A_2 è unitario, e $f(1_{A_1})=1_{A_2}$. Inoltre, se $a\in A_1$ è invertibile, anche $f(a)$ è invertibile e $f(a)^{-1}=f(a^{-1})$.

Dimostrazione: Sia $a\in A_2$. Poiché f è suriettivo, esiste $b\in A_1$ tale che $f(b)=a$. Allora

$$a=f(b)=f(b1_{A_1})=f(b)\,f(1_{A_1})=af(1_{A_1}),$$
$$a=f(b)=f(1_{A_1}b)=f(1_{A_1})\,f(b)=f(1_{A_1})a.$$

Ciò dimostra la prima parte dell'enunciato. La seconda parte è lasciata per esercizio. □

I prossimi enunciati sono analoghi a quelli di alcune proposizioni viste nella Lezione 3. Simili sono, di conseguenza, anche le dimostrazioni, che, pertanto, omettiamo.

Proposizione 5.43 *(Composizione di omomorfismi di anelli)* Siano $(A_1,+_1,\cdot_1)$, $(A_2,+_2,\cdot_2)$ e $(A_3,+_3,\cdot_3)$ anelli e siano $f:A_1\to A_2$ e $g:A_2\to A_3$ omomorfismi di anelli. Allora $g\circ f:A_1\to A_3$ è un omomorfismo di anelli.

Proposizione 5.44 *(Isomorfismi inversi)* L'applicazione inversa di un isomorfismo di anelli è un isomorfismo di anelli.

Definizione 5.45 Si dice che l'anello $(A_1,+_1,\cdot_1)$ è *isomorfo* all'anello $(A_2,+_2,\cdot_2)$ se esiste un isomorfismo di anelli $f:A_1\to A_2$. In tal caso si scrive $A_1\simeq A_2$. Scriveremo anche $A_1\overset{f}{\simeq}A_2$, quando vorremo specificare l'isomorfismo.

La precedente definizione introduce, nella classe degli anelli, una relazione binaria $\simeq$, detta di *isomorfismo.* Questa, in realtà, è una *relazione di equivalenza*.

Proposizione 5.46 *(Relazione di isomorfismo)* La relazione di isomorfismo per gli anelli è riflessiva, simmetrica e transitiva.

Come nel caso dei gruppi, la relazione di isomorfismo significa identità di struttura, che, in questo caso, si riferisce a due operazioni: anelli isomorfi sono anelli per i quali sono uguali le tavole di composizione della somma e le tavole di composizione del prodotto. In particolare si ha il seguente enunciato.

Proposizione 5.47 *(Commutatività, unitarietà e isomorfismo di anelli)* Siano $(A_1,+_1,\cdot_1)$ e $(A_2,+_2,\cdot_2)$ anelli isomorfi. Allora

(a) A_1 è commutativo se e solo se A_2 è commutativo.

(b) A_1 è unitario se e solo se A_2 è unitario.

Dimostrazione: (a) si dimostra come la Proposizione 3.16. Proviamo (b). Per ipotesi esiste un isomorfismo di anelli $f:A_1\to A_2$, che, in particolare, è un epimorfismo. Se A_1 è unitario, lo è anche A_2 in virtù della Proposizione 5.42. L'implicazione contraria si prova scambiando i ruoli di A_1 e A_2, e sostituendo f con f^{-1}. □

Osservazione 5.48 (a) Nell'Esempio 3.9 abbiamo visto che il gruppo $(\mathbb{Z},+)$ è isomorfo al suo sottogruppo H_2. Però l'anello (unitario) $(\mathbb{Z},+,\cdot)$ non è isomorfo al suo sottoanello H_2, poiché quest'ultimo non è unitario. Ciò si estende a tutti gli H_n con $n\geq 2$ (vedi Osservazione 5.27).

(b) Nella Lezione 1, abbiamo identificato ogni numero reale a con il numero complesso $(a,0)$, osservando che tale identificazione rispetta le operazioni di somma e prodotto in $\mathbb{R}$ e in $\mathbb{C}$. Secondo il linguaggio appena introdotto, ciò si traduce nella seguente affermazione: l'applicazione $f:\mathbb{R}\to\mathbb{C}$ tale che, per ogni $a\in\mathbb{R}$, $f(a)=(a,0)$, è un monomorfismo di anelli. L'anello $\mathbb{R}$ è isomorfo al sottoanello di $\mathbb{C}$ formato dai numeri complessi aventi parte immaginaria nulla.

Esercizio 5.49* Siano $(A_1,+_1,\cdot_1)$ e $(A_2,+_2,\cdot_2)$ anelli unitari, e sia $f:A_1\to A_2$ un isomorfismo di anelli. Provare che $f(\mathscr{U}(A_1))=\mathscr{U}(A_2)$ e che f induce per restrizione un isomorfismo di gruppi $f':\mathscr{U}(A_1)\to\mathscr{U}(A_2)$.

Esercizio 5.50*

(a) Provare che l'applicazione $f:\mathbb{C}\to\mathbb{C}$ definita da $z\mapsto\overline{z}$ per ogni $z\in\mathbb{C}$ è un isomorfismo di anelli.

(b) Provare che l'insieme $H=\left\{a+b\sqrt{2}\,\middle|\,a,b\in\mathbb{Q}\right\}$ è un sottoanello di $\mathbb{R}$. Dire se l'applicazione $f:H\to\mathbb{C}$ definita da $a+b\sqrt{2}\mapsto a+bi$ per ogni $a,b\in\mathbb{Q}$ è un omomorfismo di anelli.

(c) Provare che l'insieme $\mathbb{Z}[i]=\left\{a+bi\,\middle|\,a,b\in\mathbb{Z}\right\}$ è un sottoanello unitario di $\mathbb{C}$. Dire se è un campo. Dire se è un anello isomorfo a $\mathbb{Z}$.

Esercizio 5.51* Provare che ogni dominio d'integrità finito (e non banale) è un campo.