Definizione 1. Sia A un insieme non vuoto. Un'applicazione

$$* : A \times A \to A$$

si dice *legge di composizione interna* o *operazione* su A. La coppia ordinata $(A, *)$ si dice *struttura algebrica*, della quale A è il *sostegno*.

Osservazione 1. Se è assegnata una struttura algebrica $(A, *)$, allora invece di scrivere $*(x, y)$ si scrive $x * y$.

Definizione 2. Sia $(A, *)$ una struttura algebrica. Si dice che la legge di composizione $*$ verifica la proprietà *associativa* se

$$\forall x, y, z \in A, \quad (x * y) * z = x * (y * z).$$

Definizione 3. Sia $(A, *)$ una struttura algebrica. Se la legge di composizione $*$ verifica la proprietà associativa si dice che $(A, *)$ è un *monoide* (o un *semigruppo*).

Definizione 4. Sia $(A, *)$ una struttura algebrica. Si dice che $(A, *)$ ammette *elemento neutro* se

$$\exists e \in A \text{ tale che } \forall x \in A \quad x * e = e * x = x.$$

Naturalmente e si dice elemento neutro della struttura algebrica $(A, *)$.

Proposizione 1. *Se una struttura algebrica $(A, *)$ ammette elemento neutro, esso è unico.*

Dimostrazione. Siano e_1 ed e_2 elementi neutri della struttura algebrica $(A, *)$. Allora $e_1 = e_1 * e_2 = e_2$.

Osservazione 2. Nei testi spesso è chiamato monoide una struttura algebrica associativa e con elemento neutro.

Sono esempi di monoidi con unità: $(\mathbb{N}, +)$, $(\mathbb{Z}, \cdot)$, il monoide delle parole (definito a lezione).

Definizione 5. Sia $(A, *)$ una struttura algebrica dotata di elemento neutro e, e sia $x \in A$. Si dice che x è simmetrizzabile se esiste $x' \in A$ tale che $x * x' = x' * x = e$; x' si dice il *simmetrico di x*.

Definizione 6. Si dice che una struttura algebrica $(A, *)$ è un *gruppo* se è associativa, se ammette elemento neutro e se ogni elemento è simmetrizzabile. In altri termini $(A, *)$ è un gruppo se sono verificate le seguenti proprietà

- $\forall x, y, z \in A, \quad (x * y) * z = x * (y * z)$.
- $\exists e \in A$ tale che $\forall x \in A \quad x * e = e * x = x$.
- $\forall x \in a \quad \exists x' \in A$ tale che $x * x' = x' * x = e$.

Esempi di gruppi sono: $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{Q}^*, \cdot)$, $(\mathbb{R}^*, \cdot)$.

Definizione 7. Sia $(A, *)$ una struttura algebrica. Si dice che la legge di composizione $*$ verifica la proprietà *commutativa* se

$$\forall x, y \in A, \quad x * y = y * x.$$

In tal caso la struttura algebrica $(A, *)$ si dice commutativa. Un gruppo commutativo si dice *abeliano*.

Osservazione 3. Il monoide delle parole non è commutativo, mentre sono commutativi i monoidi $(\mathbb{N}, +)$, $(\mathbb{Z}, \cdot)$. I gruppi $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{Q}^*, \cdot)$, $(\mathbb{R}^*, \cdot)$ sono tutti abeliani. Si vedranno in seguito alcuni esempi di gruppi non abeliani.

Definizione 8. Sia $(A, *)$ una struttura algebrica, $\mathcal{R}$ una relazione di equivalenza su A. Si dice che $\mathcal{R}$ è *compatibile con* $*$ se

$$\forall a, b, c, d \in A, \quad ((a, b) \in \mathcal{R} \ \wedge \ (c, d) \in \mathcal{R}) \ \Rightarrow \ (a * c, b * d) \in \mathcal{R}.$$

Osservazione 4. Se una relazione di equivalenza $\mathcal{R}$ è compatibile con una legge di composizione interna $*$, allora è possibile definire sull'insieme quoziente $A/\mathcal{R}$ una legge di composizione interna $*_{\mathcal{R}}$ come segue:

$$\forall\ [a]_{\mathcal{R}}, [b]_{\mathcal{R}} \in A/\mathcal{R}, \quad [a]_{\mathcal{R}}\ *_{\mathcal{R}}\ [b]_{\mathcal{R}} = [a * b]_{\mathcal{R}}.$$

Si dimostra che $*_{\mathcal{R}}$ verifica tutte le proprietà di $*$. Quindi, in particolare, se $(A, *)$ è un monoide o un gruppo, allora $(A/\mathcal{R}, *_{\mathcal{R}})$ è monoide o un gruppo, rispettivamente. Inoltre, se $(A, *)$ è una struttura commutativa, allora anche $(A/\mathcal{R}, *_{\mathcal{R}})$ è una struttura commutativa.

Esempio 1. La congruenza ($\mathtt{mod}n$) è compatibile sia con la somma che con il prodotto di $\mathbb{Z}$ (verificato a lezione) e quindi si possono considerare le leggi di composizione interne indotte sull'insieme quoziente $\mathbb{Z}_n$.

$$\forall\ [a]_n,\ [b]_n \in \mathbb{Z}_n \quad [a]_n + [b]_n = [a+b]_n, \quad [a]_n \cdot [b]_n = [a \cdot b]_n.$$

Risultano, quindi, le due strutture algebriche $(\mathbb{Z}_n, +)$, che è un gruppo abeliano, e $(\mathbb{Z}_n, \cdot)$, che è un monoide commutativo.

Gruppi

Osservazione 5. Un gruppo G può essere denotato moltiplicativamente, per esempio con $\cdot$, con $\bullet$, con $\odot$, ecc.: in tal caso si usa generalmente la notazione 1_G o semplicemente 1 per l'elemento neutro e per ogni $x \in G$ si indica con x^{-1} l'elemento simmetrico di x, che dice *inverso di* x. Può anche essere denotato additivamente con $+$, con $\oplus$ ecc.: allora si usa generalmente la notazione 0_G o semplicemente 0 per l'elemento neutro e per ogni $x \in G$ si indica con $-x$ l'elemento simmetrico di x, che si dice *opposto di* x.

Definizione 9. Sia $(G, \cdot)$ un gruppo. Fissato $n \in \mathbb{Z}$, definisce la *potenza n-ma* di g nel modo che segue:

- ricorsivamente per $n \in \mathbb{N}$:
$$\begin{cases} g^0 = 1_G \\ g^n = g^{n-1} g, \quad n > 0 \end{cases}$$
- per $n < 0$, si pone $g^n = (g^{-n})^{-1}$.

Osservazione 6. Se $(G, +)$ è un gruppo denotato additivamente, allora fissato $n \in \mathbb{Z}$, si parla non di potenza n-ma di g, ma di *multiplo secondo* n di g. Si definisce in modo analogo:

- ricorsivamente per $n \in \mathbb{N}$:
$$\begin{cases} 0\ g = 0 \\ n\ g = (n-1)\ g + g, \quad n > 0 \end{cases}$$
- per $n < 0$, si pone $n\ g = -(-n\ g)$.

Proposizione 2. *Sia $(G, \cdot)$ un gruppo. Allora si ha*

(1) $\forall g \in G, \quad \forall m, n \in \mathbb{Z} \quad g^m \cdot g^n = g^{m+n}$
(2) $\forall g \in G, \quad \forall m, n \in \mathbb{Z} \quad (g^m)^n = g^{mn}$
(3) *se $(G, \cdot)$ è abeliano, allora* $\forall g, h \in G, \quad \forall n \in \mathbb{Z} \quad (g \cdot h)^n = g^n \cdot h^n$.

Osservazione 7. Se il gruppo $(G, +)$ è denotato additivamente, allora le precedenti proprietà si riscrivono nel modo seguente:

(1) $\forall g \in G, \quad \forall m, n \in \mathbb{Z} \quad (m+n)\ g = m\ g + n\ g$
(2) $\forall g \in G, \quad \forall m, n \in \mathbb{Z} \quad m\ (n\ g) = (mn)\ g$
(3) se $(G, +)$ è abeliano, allora $\forall g, h \in G, \quad \forall n \in \mathbb{Z} \quad n\ (g + h) = n\ g + n\ h$.

Definizione 10. Sia $(G, \cdot)$ un gruppo, $H \subseteq G$. Si dice che H è un *sottogruppo* di G se verifica le seguenti 3 condizioni

SG_1) $H \neq \emptyset$
SG_2) $\forall x, y \in H, \quad x \cdot y \in H$
SG_3) $\forall x \in H, \quad x^{-1} \in H$.

Osservazione 8. Nel caso di un gruppo $(G, +)$ denotato additivamente, le condizioni SG_2), SG_3) della precedente Definizione si riscrivono come segue:

SG_2) $\forall x, y \in H, \quad x + y \in H$
SG_3) $\forall x \in H, \quad -x \in H$.

Teorema 1. *Sia $(G, \cdot)$ un gruppo, $H \subseteq G$. Allora H è un sottogruppo di G se e soltanto se sono verificate le seguenti 2 condizioni*

SG'$_1$) $1_G \in H$
SG'$_2$) $\forall x, y \in H, \quad x \cdot y^{-1} \in H$.

Osservazione 9. Nel caso di un gruppo $(G, +)$ denotato additivamente, le condizioni SG'$_1$), SG'$_2$) del precedente Teorema si riscrivono come segue:

SG_2) $0_G \in H$
SG_3) $\forall x, y \in H, \quad x - y \in H$.

Esempio 2. Sia $(G, \cdot)$ un gruppo. Allora G e $\{1_G\}$ sono sottogruppi di $(G, \cdot)$.

Proposizione 3. *Sia $(G, \cdot)$ un gruppo. Allora l'intersezione di due sottogruppi di G è un sottogruppo di G (si verifichi per esercizio).*

Osservazione 10. In generale l'unione di due sottogruppi di G non è un sottogruppo di G: ciò si può vedere con degli esempi.

Definizione 11. Sia $(G, \cdot)$ un gruppo. Si indica con $|G|$ la cadinalità (finita o infinita di G), che si chiama *ordine* di G. La stessa notazione vale ovviamente per i sottogruppi.

Teorema 2. *(Lagrange) Sia $(G, \cdot)$ un gruppo finito di ordine n, H un suo sottogruppo di ordine h. Allora $h|n$ (h è un divisore di n).*

Proposizione 4. Sia $(G, \cdot)$ un gruppo, $g \in G$. Allora il sottoinsieme

$$< g >= \{a \in G : \exists h \in \mathbb{Z} \text{ tale che } a = g^h\} = \{g^h : h \in \mathbb{Z}\}$$

è un sottogruppo di G.
(verificata a lezione)

Definizione 12. Sia $(G, \cdot)$ un gruppo, $g \in G$. Il sottogruppo $< g >$ si dice *sottogruppo ciclico generato da g.*

Osservazione 11. Se il gruppo $(G, +)$ è denotato additivamente e $g \in G$, allora il sottogruppo ciclico generato da g si scrive

$$< g >= \{a \in G : \exists h \in \mathbb{Z} \text{ tale che } a = hg\} = \{hg \mid h \in \mathbb{Z}\}.$$

Osservazione 12. Si osservi che un gruppo infinito può anche ammettere sottogruppi finiti: per esempio il sottogruppo ciclico di $(\mathbb{Q}^*, \cdot)$ generato da -1 è finito in quanto $< -1 >= \{1, -1\}$.

Proposizione 5. *Sia $(G, \cdot)$ un gruppo, $g \in G$. Allora si ha una delle seguenti possibilità:*

(1) $(\forall\ h, k \in \mathbb{Z})\ (g^h \neq g^k) \ \Leftrightarrow < g >$ *è infinito*
(2) $(\exists\ h, k \in \mathbb{Z})\ (g^h = g^k) \ \Leftrightarrow < g >$ *è finito.*

Definizione 13. Sia $(G, \cdot)$ un gruppo, $g \in G$. Si dice che g *ha ordine infinito*, e si scrive $|g| = +\infty$, se $| < g > | = +\infty$; si dice che g *ha ordine o periodo* $k \in \mathbb{N}^*$, e si scrive $|g| = k$, se $| < g > | = k$. (Si noti che in ogni caso $|g| = | < g > |$.)

Definizione 14. Si dice che un gruppo $(G, \cdot)$ è *ciclico* se esiste $g \in G$ tale che $< g >= G$. In tal caso g si dice *generatore* di G.

Osservazione 13. Sia $(G, \cdot)$ un gruppo finito di ordine n. Allora $(G, \cdot)$ è ciclico se e solo se esiste un elemento $g \in G$ tale che $|g| = n$.

Esempio 3. Sono gruppi ciclici:

(1) $(\mathbb{Z}, +)$, in quanto 1 e -1 ne sono generatori
(2) $(\mathbb{Z}_n, +)$, in quanto $[1]_n$ ne è generatore.

Teorema 3. *Ogni sottogruppo di un gruppo ciclico è ciclico.*

Quindi, per esempio, sono ciclici tutti i sottogruppi di $(\mathbb{Z}, +)$ e tutti i sottogruppi di $(\mathbb{Z}_n, +)$

Teorema 4. *(Inverso del Teorema di Lagrange per i gruppi ciclici) Sia $(G, \cdot)$ un gruppo ciclico di ordine n. Allora per ogni h divisore di n esiste un unico sottogruppo di $(G, \cdot)$ avente ordine h.*

Proposizione 6. *Sia $(G, \cdot)$ un gruppo ciclico finito di ordine n e ne sia g un generatore, ovvero $G =< g >$. Pertanto, per ogni elemento $a \in G$ esiste $h \in \mathbb{Z}$ tale che $a = g^h$. Risulta allora:*

$$|a| = |g^h| = \frac{n}{M.C.D.(h, n)} \tag{1}$$

Osservazione 14. Segue da (1) che per ogni numero intero h primo con n, g^h è un generatore di G. In particolare, i generatori del gruppo $(\mathbb{Z}_n, +)$ sono tutti e soli gli elementi $[h]_n \in \mathbb{Z}_n$ tali che h sia primo con n e quindi i generatori di $(\mathbb{Z}_n, +)$ sono esattamente $\varphi(n)$ (φ funzione di Eulero).

Esercizio 1. Verificare che:

1. un gruppo finito di ordine p primo è ciclico.
2. un gruppo ciclico è abeliano.

Proposizione 7. *Siano $(G, \cdot)$ un gruppo, $a \in G$, con $|a| = m$. Allora si ha:*

$$m = min\{h \in \mathbb{N}^* : a^h = 1_G\}$$

Proposizione 8. *Sia $n \in \mathbb{N}$, $n > 1$. Allora un elemento $[a]_n \in \mathbb{Z}_n^*$ è invertibile nel monoide $(\mathbb{Z}_n, \cdot)$ se e soltanto se $M.C.D.(a, n) = 1$.*

Dimostrazione. Un elemento $[a]_n \in \mathbb{Z}_n^*$ è invertibile se esiste $[x]_n \in \mathbb{Z}_n$ tale che

$$[a]_n \cdot [x]_n = [1]_n,$$

ovvero

$$[a \cdot x]_n = [1]_n.$$

Pertanto, per trovare $[x]_n$, laddove esista, bisogna risolvere la congruenza lineare

$$a\ x \equiv 1\ (\texttt{mod}\ n), \tag{2}$$

che ha soluzioni se e solo se $M.C.D.(a, n)|1$. Inoltre, nel caso in cui (2) abbia soluzioni, ce nè soltanto una $\texttt{mod}\ n$. Questo a conferma dell'unicità dell'inverso.

Corollario 1. *Se $p \in \mathbb{Z}$ è un numero primo, allora $\mathbb{Z}_p^*$ è chiuso rispetto a $\cdot$.*

Dimostrazione. Per la proposizione precedente, ogni elemento di $\mathbb{Z}_p^*$ ha inverso rispetto a $\cdot$. Siano $[a]_p,\ [b]_p \in \mathbb{Z}_p^*$ se fosse

$$[a]_p \cdot [b]_p = 0,$$

moltiplicando a sinistra per l'inverso $[a]_p^{-1}$ di $[a]_p$ si avrebbe

$$[a]_p^{-1} \cdot [a]_p \cdot [b]_p = [a]_p^{-1} \cdot 0,$$

ossia $[b]_p = 0$ che contraddice $[b]_p \in \mathbb{Z}_p^*$. Quindi $[a]_p \cdot [b]_p \in \mathbb{Z}_p^*$, ovvero $\mathbb{Z}_p^*$ è chiuso rispetto a $\cdot$.

Corollario 2. *Se $p \in \mathbb{Z}$ è un numero primo, allora la struttura algebrica $(\mathbb{Z}_p^*, \cdot)$ è un gruppo abeliano.*

Un esempio di gruppo non abeliano si costruisce nel modo che segue. Sia A un insieme e sia $\mathcal{S}(A)$ l'insieme delle applicazioni bigettive su A. Si prova facilmente che la struttura algebrica $(\mathcal{S}(A), \circ)$ è un gruppo non abeliano (dimostrato a lezione).
Sia S_n l'insieme delle permutazioni su n oggetti, ovvero su un insieme di cardinalità n. Non è lesivo della generalità considerare S_n come l'insieme delle permutazioni sui primi numeri naturali non nulli

$$\{1, 2, \ldots, n\}.$$

Si è visto che $|S_n| = n!$. La composizione di applicazioni fornisce una legge di composizione interna su S_n:

$$\circ : S_n \times S_n \to S_n.$$

$(S_n, \circ)$ è un gruppo, (è un caso particolare di $(\mathcal{S}(A), \circ)$) e per $n > 2$ è *non* abeliano. Quindi non può essere ciclico per $n > 2$ (cf. Esercizio 1).

Definizione 15. Si sice che una permutazione f *muove* un elemento a se $f(a) \neq a$; si dice che *fissa* a se $f(a) = a$.

Definizione 16. Si dice che due permutazioni f e g sono *disgiunte* se gli elementi mossi da f sono fissati da g.

Osservazione 15. Se due permutazioni f e g sono disgiunte, allora

$$f \circ g = g \circ f.$$

Definizione 17. Si dice *ciclo di lunghezza* r, e si indica con il simbolo $(c_1 c_2 \ldots c_r)$, $r \leq n$ la permutazione $f \in S_n$ tale che

$$f(c_1) = c_2, f(c_2) = c_3, \ldots, f(c_{r-1}) = c_r, f(c_r) = c_1$$

e tutti gli altri elementi vengono fissati da f. Un ciclo di lunghezza 2 si chiama scambio.

Osservazione 16. Si osservi che si ha $(c_1 c_2 \ldots c_r) = (c_2 \ldots c_r c_1) = (c_3 \ldots c_r c_1 c_2) = \ldots (c_r c_1 \ldots c_{r-1})$.

Teorema 5. Sia $f \in S_n$. Allora f è un ciclo oppure può essere scritta, in modo unico a meno dell'ordine, come prodotto di cicli disgiunti.

Osservazione 17. Si può scrivere il ciclo $(c_1 c_2 \ldots c_r)$ come

$$(c_1 c_2 \ldots c_r) = (c_1 c_r) \circ \cdots \circ (c_1 c_3) \circ (c_1 c_2).$$

Quindi ogni ciclo può essere scritto come prodotto di scambi e dunque ogni permutazione può essere scritta prima come prodotto di cicli e poi come prodotto di scambi. La scomposizione in scambi non è unica. Per esempio:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 2 & 5 & 4 \end{pmatrix} = (1\ 3\ 2) \circ (4\ 5) = (1\ 2) \circ (1\ 3) \circ (4\ 5)$$
$$= (1\ 2) \circ (3\ 4) \circ (3\ 4) \circ (1\ 3) \circ (4\ 5).$$

Teorema 6. Due scomposizioni in scambi di una stessa permutazione hanno la stessa parità.

Il precedente Teorema giustifica la seguente:

Definizione 18. Si dice che una permutazione è *di classe pari* (rispettivamente *di classe dispari*) se una sua qualunque scomposizione è costituita da un numero pari (rispettivamente dispari) di scambi.

Si può quindi definire l'applicazione

$$\Delta : S_n \to \{+1, -1\} \text{ tale che } \Delta(f) = \begin{cases} 1 & \text{se } f \text{ è di classe pari} \\ -1 & \text{se } f \text{ è di classe dispari.} \end{cases}$$

Proposizione 9. Il sottoinsieme formato dalle permutazioni di classe pari costituisce un sottogruppo di S_n, che si chiama gruppo alterno.

Osservazione 18. Sia σ un ciclo di lunghezza r. Allora l'ordine di σ nel gruppo $(S_n, \circ)$ è r.

Proposizione 10. *Sia $f \in S_n$, e sia $f = \sigma_1 \circ \cdots \circ \sigma_h$ la sua scomposizione in cicli disgiunti. Allora*

$$|f| = m.c.m.(|\sigma_1|, \ldots, |\sigma_h|).$$

Osservazione 19. Il gruppo $(S_n, \circ)$ non è ciclico per $n \geq 3$.

Definizione 19. Siano $(A, *)$, $(B, \cdot)$ due strutture algebriche. Si può allora considerare sul prodotto cartesiano $A \times B$ la legge di composizione interna $\odot$ definita come segue:

$$\forall (a, b),\ (a', b') \in A \times B, \quad (a, b) \odot (a', b') = (a * a', b \cdot b'). \tag{3}$$

Si può verificare facilmente la seguente:

Proposizione 11. *Siano $(A, *)$, $(B, \cdot)$ due strutture algebriche, e sia $(A \times B, \odot)$ la struttura algebrica definita in* (3)*. Allora si ha:*

- *se le due strutture $(A, *)$ e $(B, \cdot)$ sono entrambe associative, allora $(A \times B, \odot)$ è associativa*
- *se la struttura $(A, *)$ ammette elemento neutro e_A e la struttura $(B, \cdot)$ ammette elemento neutro e_B allora $(A \times B, \odot)$ ammette elemento neutro (e_A, e_B)*
- *se a è un elemento simmetrizzabile di A avente a' come simmetrico e b è un elemento simmetrizzabile di B avente b' come inverso, allora la coppia (a, b) è simmetrizzabile in $(A \times B, \odot)$ ed ha come simmetrico (a', b')*
- *se le due strutture $(A, *)$ e $(B, \cdot)$ sono commutative, allora $(A \times B, \odot)$ è commutativa*
- *quindi, se $(A, *)$ e $(B, \cdot)$ sono monoidi (commutativi), allora $(A \times B, \odot)$ è un monoide (commutativo); se $(A, *)$ e $(B, \cdot)$ sono gruppi (abeliani), allora $(A \times B, \odot)$ è un gruppo (abeliano), che si dice* gruppo somma diretta *dei gruppi $(A, *)$ e $(B, \cdot)$, che si indica con $A \oplus B$.*

Osservazione 20. Si può verificare che se $(A, *)$ e $(B, \cdot)$ sono gruppi, $a \in A$, $b \in B$, entrambi di ordine finito, allora si ha la seguente formula nel gruppo somma diretta $A \oplus B$

$$|(a, b)| = m.c.m(|a|, |b|).$$

Esempio 4. Fissati $n, m \in \mathbb{N}^*$, $n \neq 1$, si può considerare il gruppo somma diretta $\mathbb{Z}_n \oplus \mathbb{Z}_m$ di $(\mathbb{Z}_n, +)$ e $(\mathbb{Z}_m, +)$, che è un gruppo abeliano finito di ordine $n \cdot m$.

Esercizio 2. In quali ipotesi su n ed m, $\mathbb{Z}_n \oplus \mathbb{Z}_m$ è ciclico?

Esercizio 3. Studiare il gruppo $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ (gruppo di Klein).

Anelli

Definizione 20. Sia A un insieme non vuoto, dotato di due leggi di composizione interne $+$ e $\cdot$. Si dice che la struttura algebrica $(A, +, \cdot)$ è un *anello* se;

(1) $(A, +)$ è un gruppo abeliano
(2) $(A, \cdot)$ è un monoide (ovvero $\cdot$ è associativa)
(3) valgono le proprietà distibutive, ovvero $\forall a, b, c \in A$ si ha

$$a \cdot (b + c) = a \cdot b + a \cdot c \quad (a + b) \cdot c = a \cdot c + b \cdot c.$$

Se $(A, \cdot)$ è un monoide con unità, allora si parla di *anello con unità*; se $(A, \cdot)$ è commutativo, allora $(A, +, \cdot)$ si dice *anello commutativo.*

Nel seguito ci si riferirà sempre ad anelli con unità, anche se verranno chiamati semplicemente anelli.

Esempio 5. Sono esempi di anelli commutativi gli insiemi $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Z}_n, +, \cdot)$.

Tra le proprietà di un anello , che per ragioni di tempo vengono tralasciate, si evidenzia la seguente:

Proposizione 12. *Sia $(A, +, \cdot)$ un anello. Allora si ha:*

$$\forall\ a \in A \quad a \cdot 0 = 0 \cdot a = 0.$$

Dimostrazione. Sia $A \in A$. Per la proprietà distributiva, si ha:

$$a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 + a \cdot 0$$

e, per le leggi di cancellazione applicate al gruppo $(A, +)$, segue $a \cdot 0 = 0$; analogamente si vede che $0 \cdot a = 0$.

Definizione 21. Si dice che un anello $(A, +, \cdot)$ è un *corpo* se ogni elemento non nullo di A è invertibile rispetto a $\cdot$; un corpo commutativo si chiama *campo.*

Esempio 6. Sono campi, per esempio, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{Z}_p, +, \cdot)$, p numero primo.

Osservazione 21. Nell'anello $(\mathbb{Z}_6, +, \cdot)$ il prodotto $[3]_6 \cdot [2]_6 = [0]_6$, pur essendo $[3]_6 \neq [0]_6$ e $[2]_6 \neq [0]_6$; d'altra parte $[5]_6$ ammette come inverso moltiplicativo $[5]_6$. Pertanto hanno senso le seguenti definizioni:

Definizione 22. Sia $(A, +, \cdot)$ un anello. Un elemento $a \in A$ si dice *divisore dello zero* se

(1) $a \neq 0$
(2) $\exists\ b \in A,\ b \neq 0,$ tale che $a \cdot b = 0.$

In tal caso b si dice *codivisore dello zero* di a

Osservazione 22. Si noti che un divisore dello zero di un anello in generale ammette più di un codivisore dello zero: nell'anello $(\mathbb{Z}_6, +, \cdot)$, si può notare che $[2]_6$ e $[4]_6$ sono entrambi codivisori dello zero di $[3]_6$.

Definizione 23. Sia $(A, +, \cdot)$ un anello. Un elemento $a \in A$ si dice *unitario* se è inveritibile rispetto a $\cdot$.

Proposizione 13. *Sia $(A, +, \cdot)$ un anello. Allora un elemento unitario di A non può essere un divisore dello zero.*

Dimostrazione. Sia $a \in A$ un elemento unitario. Se per assurdo a fosse un divisore dello zero, sarebbe $a \neq 0$ ed inoltre esisterebbe $b \in A$, $b \neq 0$ tale che

$$a \cdot b = 0. \tag{4}$$

Moltiplicando per a^{-1}, da (4) si avrebbe

$$a^{-1} \cdot (a \cdot b) = a^{-1} \cdot 0 = 0$$

ovvero, per l'associatività di $\cdot$,

$$b = (a^{-1} \cdot a) \cdot b = 0$$

che dà luogo a contraddizione.

Segue immediatamente il:

Corollario 3. *In un campo non ci sono divisori dello zero.*

Osservazione 23. L'anello $(\mathbb{Z}, +, \cdot)$ non ha divisori dello zero: per questo motivo si chiama *dominio di integrità*.

Osservazione 24. Si dimostra che in un anello *finito* ogni elemento non nullo è divisore dello zero oppure è unitario. Per esempio si è osservato (Proposizione 8) che in $\mathbb{Z}_n$, n non primo, sono unitari gli elementi primi con n e quindi gli elementi unitari sono in numero di $\varphi(n)$ (φ funzione di Eulero); i rimanenti $n - 1 - \varphi(n)$ elementi non nulli di $\mathbb{Z}_n$ sono quindi divisori dello zero.