Gruppi, anelli, campi e polinomi: le prime definizioni.

Ilaria Del Corso

1 GRUPPI

Definizione 1.1.

Sia G un insieme, $G \neq \varnothing$ e sia $*$ un'operazione su G. Si dice che $(G, *)$ è un **gruppo** se

1. $*$ è associativa, ossia $\forall a, b, c \in G, \quad (a * b) * c = a * (b * c)$.
2. Esiste un elemento neutro, ossia $\exists e \in G$ tale che $g * e = e * g = g \ \ \forall g \in G$.
3. Esiste l'inverso di ogni el., ossia: $\forall g \in G \quad \exists g^{-1} \in G$ tale che $g * g^{-1} = g^{-1} * g = e$.

Definizione 1.2.

Un gruppo $(G, *)$ si dice **abeliano** se $*$ è commutativa, cioè $\forall g, h \in G, \quad g * h = h * g$.

Osservazione 1.3.

Per verificare che un insieme non vuoto è un gruppo occorre fare anche la verifica che $*$ sia un'operazione su G, cioè che $\forall g, h \in G \ \ g * h \in G$

Esempio 1.4.

1. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ sono gruppi abeliani rispetto alla somma $+$
2. $(\mathbb{N}, +)$ non è un gruppo.
3. $(\mathbb{Z}, \cdot)$ non è un gruppo.
4. $(\mathbb{Q}^*, \cdot)$ è un gruppo.
5. $(\{x \in \mathbb{C} \mid x^n = 1\}, \cdot)$ è un gruppo.
6. $(\{f : X \longrightarrow X \mid f \text{ è bigettiva}\}, \circ)$ è un gruppo.
7. $(\mathbb{Z}/m\mathbb{Z}, +)$ è un gruppo.
8. $\cdot$ è un'operazione su $\mathbb{Z}/m\mathbb{Z}$ ma $(\mathbb{Z}/m\mathbb{Z}, \cdot)$ non è un gruppo.
9. $(\mathbb{Z}/m\mathbb{Z}^*, \cdot)$ è un gruppo per ogni m.

2 ANELLI

Definizione 2.1.

Sia A un insieme su cui sono definite due operazioni $+, \cdot$.
$(A, +, \cdot)$ si dice **Anello** se

$(A, +)$ è un gruppo abeliano

$\cdot$ è associativa

valgono le leggi distributive, cioè se $\forall a, b, c \in A$ si ha $(a + b)c = ac + bc$ e $a(b + c) = ab + ac$.

Definizione 2.2.

Un anello A si dice **Commutativo** se l'operazione $\cdot$ è commutativa.
Si dice **con identità** se $\exists$ l'identità dell'operazione $\cdot$, cioè se $\exists 1 \in A$ tale che $a \cdot 1 = 1 \cdot a = 1 \quad \forall a \in A$.

Nel seguito, senza ulteriormente specificarlo, A indicherà un anello commutativo con identità.

Definizione 2.3.

Sia A un anello. $a \in A$ si dice **invertibile** se $\exists a' \in A$ tale che $aa' = a'a = 1$.
Denotiamo con A^* l'insieme degli elementi invertibili di A .

Esempio 2.4.

1. $(\mathbb{Z}, +, \cdot), (\mathbb{Q}, +, \cdot), (\mathbb{R}, +, \cdot), (\mathbb{C}, +, \cdot)$ sono anelli commutativi con identità.
2. $(\mathbb{Z}/m\mathbb{Z}, +, \cdot)$ è un anello commutativo con identità.
   Sappiamo già che gli elementi invertibili sono $\mathbb{Z}/m\mathbb{Z}^* = \{[a] \mid (a, m) = 1\}$.
3. $M_{n\times n}(\mathbb{R})$ con le usuali operazioni di somma e prodotto tra le matrici è un anello (non commutativo se $n \geq 2$).

Proposizione 2.5.

Sia A un anello. Allora $\forall a \in A$ si ha $a0 = 0$.

Dimostrazione.

$a0 = a(0 + 0) = a0 + a0$, da cui, sottraendo da entrambi i membri $a0$, si ottiene $a0 = 0$. ▲

Definizione 2.6.

Un anello commutativo con identità K si dice **campo** se ogni suo elemento diverso da 0 è invertibile, cioè se $K^* = K \setminus \{0\}$.

Osservazione 2.7. Sia K è un campo allora $K \setminus \{0\}$ è un gruppo abeliano rispetto al prodotto. Inoltre in un campo vale la **legge d'annullamento del prodotto**, coiè

$$ab = 0 \Rightarrow a = 0 \vee b = 0.$$

Per dimostrarlo basta osservare che se se $a = 0$ siamo a posto. Se invece $a \neq 0$, allora a è invertibile (in un campo infatti tutti gli elementi diversi da 0 sono invertibili) e se a' è l'inverso di a allora $a'a = 1$, quindi $b = 1b = (a'a)b = a'(ab) = a'0 = 0$.

Esempio 2.8.

1. $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ sono campi che hanno infiniti elementi.
2. Se p è un numero primo $\mathbb{Z}/p\mathbb{Z}$ è un campo con p elementi.

POLINOMI

Sia K un campo e x una indeterminata.

L'anello dei polinomi con coefficienti in K nella indeterminata x è l'insieme

$$K[x] := \{a_0 + a_1x + \cdots + a_nx^n \mid a_i \in K,\ n \in \mathbb{N}\}.$$

Definizione 2.9.

Siano $f(x) = \sum_{i=0}^{n} a_ix^i$, $g(x) = \sum_{j=0}^{m} b_jx^j \in K[x]$.
Poniamo

$$f(x) + g(x) := \sum_{i=0}^{n}(a_i + b_i)x^i$$

(dove abbiamo supposto $n \geq m$ e abbiamo posto $b_{m+1} = \cdots = b_n = 0$), e

$$f(x) \cdot g(x) := \sum_{h=0}^{n+m}(\sum_{i+j=h} a_ib_j)x^h.$$

Teorema 2.10.

$(K[x], +, \cdot)$ è un anello commutativo con identità.

Dimostrazione.

Si verificano le varie proprietà sfruttando le analoghe per K . ▲

Definizione 2.11.

Sia $f(x) = \sum_{i=0}^{n} a_ix^i \in K[x] \setminus \{0\}$. Definiamo il **grado** di f nel seguente modo:

$$\deg f := \max\{i \in \mathbb{N} \mid a_i \neq 0\}$$

Scegliamo di non definire il grado del polinomio 0 .

Proposizione 2.12.

Sia K un campo e siano $f, g \in K[x] \setminus \{0\}$. Allora

1. $\deg(fg) = \deg f + \deg g$;
2. $\deg(f+g) \leq \max\{\deg f, \deg g\}$.

DIMOSTRAZIONE.

Siano $f = \sum_{i=0}^{n} a_i x^i$ e $g = \sum_{j=0}^{m} b_j x^j$ con $a_n \neq 0$ e $b_m \neq 0$.
Poiché K è un campo, si ha $a_n b_m \neq 0$, quindi $f(x)g(x) = a_n b_m x^{n+m} +$ termini di grado più basso, cioè $\deg(fg) = n + m = \deg f(x) + \deg g(x)$.

Dalla definizione di $f+g$ segue l'enunciato 2 (il $<$ si ha nel caso in cui il monomio di grado massimo di g sia l'opposto del monomio di grado massimo di f). ▲

Corollario 2.13.

Gli elemeti invertibili di $K[x]$ sono le costanti diverse da 0.

DIMOSTRAZIONE.

Chiaramente tutte le costanti diverse da 0 sono invertibili perché lo sono già in K.

Viceversa se $f(x) \in K[x]$ è invertibile allora $\exists g(x) \in K[x]$ tale che $f(x)g(x) = 1$. Passando ai gradi

$$0 = \deg(fg) = \deg f + \deg g.$$

Quindi $\deg f = \deg g = 0$, cioè $f \in K^*$. ▲

L'anello $K[x]$ è per molti aspetti somigliante all'anello $\mathbb{Z}$. In questa somiglianza il grado gioca il ruolo che il valore assoluto ha in $\mathbb{Z}$.

Teorema 2.14. (Teorema di divisione euclidea).

Siano $f, g \in K[x]$, con $f \neq 0$. Allora esistono e sono unici $q, r \in K[x]$ tali che $g = qf + r$ con $r = 0$ oppure $\deg r < \deg f$.

DIMOSTRAZIONE.

Esistenza: Se $g = 0$ allora $q = r = 0$. Supponiamo quindi $g \neq 0$ e dimostriamo l'asserto per induzione sul grado di g.

Se $\deg g = 0$ e $\deg f = 0$ allora $g = f\left(\frac{g}{f}\right) + 0$.

Se $\deg g < \deg f$ allora $g = 0f + g$, quindi $r = g$ e $q = 0$.

Sia quindi $m = \deg g \geq \deg f = n$ e $f = \sum_{i=0}^{n} a_i x^i$ e $g = \sum_{j=0}^{m} b_j x^j$.

Pongo

$$g_1(x) = g(x) - \underset{\|}{\frac{b_m}{a_n} x^{m-n} f(x)}$$
$$b_m x^m + \dots$$

Allora $\deg g_1 < m$. Quindi per induzione

$$g_1(x) = q(x)f(x) + r(x) \text{ con } r = 0 \text{ opp. } \deg r < \deg f$$

$$\Rightarrow g(x) = g_1(x) + \frac{b_m}{a_n}x^{m-n}f(x) = \left(q + \frac{b_m}{a_n}x^{m-n}\right)f(x) + r(x).$$

Unicità: Sia $g = qf + r = q_1 f + r_1$; allora $(q_1 - q)f = r - r_1$ se i due membri non fossero 0, guardando i gradi si avrebbe un assurdo. ▲

Definizione 2.15.

Siano $f, g \in K[x]$, si dice che f divide g (in simboli $f \mid g$) se $g(x) = f(x)q(x)$.

Teorema 2.16. (Teorema di Ruffini).

Siano $f \in K[x]$ e $a \in K$. Allora

$$f(a) = 0 \Longleftrightarrow x - a \mid f(x)$$

Dimostrazione.

Sia $f(x) = (x - a)q(x) + r$, allora, poichè $\deg(r) < \deg(x - a) = 1$, r è una costante. Valutando in a l'espressione di $f(x)$ otteniamo $f(a) = r$, quindi $r = 0 \Leftrightarrow f(a) = 0$. ▲

Corollario 2.17.

Sia $f \in K[x] \setminus \{0\}$, allora f ha al più $\deg f$ radici distinte in K .

Dimostrazione.

Per induzione su $n = \deg f$.

Se $n = 0$, il polinomio f è costante e non nullo e quindi non ha radici.

Supponiamo vera la tesi per polinomi di grado $n - 1$.

Se f non ha radici vale la tesi. Sia $\alpha \in K$ una radice di $f(x)$, allora $f(x) = (x - \alpha)f_1(x)$ con $\deg f_1(x) = n - 1$ e per l'ipotesi induttiva ha al più $n - 1$ radici in K . Poiché $\forall \beta \neq \alpha$ tale che $f(\beta) = (\beta - \alpha)f_1(\beta) = 0$ si ha $f_1(\beta) = 0$, si ha la tesi. ▲

Definizione 2.18.

Siano $f, g \in K[x]$ non entrambi nulli. Un polinomio $d(x) \in K[x]$ è un **massimo comune divisore** tra f e g se

1. $d(x) \mid f(x)$ e $d(x) \mid g(x)$,
2. $\forall p(x)$ tale che $p(x) \mid f(x)$ e $p(x) \mid g(x)$, si ha $p(x) \mid d(x)$.

Teorema 2.19. (Esistenza e unicità del MCD **)**

Siano $f, g \in K[x]$ non entrambi nulli, allora esiste un loro massimo comune divisore $d(x)$ e si può trovare con l'algoritmo euclideo.

Inoltre $\exists a(x), b(x) \in K[x]$ tali che

$$d(x) = a(x)f(x) + b(x)g(x).$$

Infine $d_1(x)$ è un massimo comune divisore tra $a(x)$ e $b(x)$ se e solo se $d_1(x) = c \cdot d(x)$ con $c \in K^*$.

Dimostrazione.

La dimostrazione segue la stessa linea di quella per gli interi. ▲

Fattorizzazione di polinomi

Definizione 2.20.

Sia $f \in K[x]$ un polinomio non costante. f si dice **irriducibile** se

$$f = gh \Rightarrow g \in K[x]^* = K^* \vee h \in K^*.$$

Definizione 2.21.

$f(x) \in K[x]$ non costante si dice **primo** se $f(x) \mid g(x)h(x)$ implica $f \mid g$ oppure $f \mid h$.

Proposizione 2.22.

Sia $f \in K[x]$. Allora f è irriducibile $\Leftrightarrow$ f è primo.

Dimostrazione.

La dimostrazione è identica a quella fatta per gli interi. ▲

Teorema 2.23.

Ogni polinomio $f \in K[x]$ non costante si fattorizza in modo "unico" come prodotto di polinomi irriducibili.

Dimostrazione.

Anche in questo caso la dimostrazione è analoga a quella fatta per gli interi, e quindi la omettiamo. ▲

Osservazione 2.24.

Nel teorema precedente "unico" vuol dire a meno dell'ordine e di moltiplicazione dei fattori per costanti $\neq 0$. In particolare in $\mathbb{Q}[x]$ si ha ad esempio che

$$(x-1)(x+1) \text{ e } (\frac{1}{2}x - \frac{1}{2})(2x-2)$$

sono considerate fattorizzazioni equivalenti del polinomio $x^2 - 1$.

Corollario 2.25.

$f \in K[x]$, $f \neq 0$ ha al più $\deg f$ radici in K contate con molteplicità.

Teorema fondamentale dell'algebra e sue conseguenze.

Teorema 2.26. (Teorema fondamentale dell'algebra).

Ogni polinomio $p(x) \in \mathbb{C}[x]$ con $\deg p \geq 1$ ha almeno una radice in $\mathbb{C}$.

(Non dimostriamo questo teorema).

Conseguenze:

1. $p(x) \in \mathbb{C}[x]$ è irriducibile $\Leftrightarrow \deg p(x) = 1$.

   ($\Leftarrow$ ovvio;

   $\Rightarrow$ Se $\deg p(x) = n > 1$ allora $\exists \alpha \in \mathbb{C}$ tale che $p(\alpha) = 0$, quindi dal teorema di Ruffini si ha $p(x) = (x - \alpha)p_1(x)$ con $\deg p_1 = n - 1 > 0$, quindi $p_1(x)$ non invertibile. Ne segue che quello esibito è uno spezzamento di $p(x)$ che ne mostra la riducibilità.

2. Ogni polinomio di $\mathbb{C}[x]$ si fattorizza come prodotto di polinomi di primo grado.

3. $\forall p(x) \in \mathbb{C}[x]$ $\deg p(x) = n \Rightarrow p$ ha esattamente n radici in $\mathbb{C}$ (contate con molteplicità).

4. $f(x) \in \mathbb{R}[x]$ è irriducibile $\Leftrightarrow$ $\deg f = 1$ oppure $\deg f = 2$ e $\Delta_f < 2$.

   (Sia $\deg f(x) = n$; poiché $\mathbb{R} \subset \mathbb{C}$, guardiamo al polinomio $f(x)$ come polinomio di $\mathbb{C}[x]$. Per il punto 3 si ha: $f(x) = c(x - \alpha_1) \cdots (x - \alpha_n)$. D'altra parte, poiché $f(x) \in \mathbb{R}[x]$ si ha $f = \overline{f}$, dove $\overline{\ }$ indica il complesso coniugato. Quindi,

   $$f(x) = \overline{f(x)} = c(x - \overline{\alpha_1}) \cdots (x - \overline{\alpha_n}),$$

   da cui, per il Teorema di fattorizzazione unica, si ha $\{\alpha_i\} = \{\overline{\alpha_i}\}$.

   Ne segue che per ogni i , esiste un indice j tale che $\overline{\alpha_i} = \alpha_j$. Vale $\overline{\alpha_i} = \alpha_i \iff \alpha_i \in \mathbb{R}$; quindi se $\alpha_i \notin \mathbb{R}$ oppure $\exists j \neq i$ tale che $\overline{\alpha_i} = \alpha_j$ e in tal caso

   $$(x - \alpha_i)(x - \overline{\alpha_i}) = x^2 - 2\,\mathrm{Re}(\alpha_i)x + |\alpha_i|^2$$

   è un polinomio con coefficienti reali e $\Delta < 0$.

   Questo mostra che che i fattori irriducibili di un qualsiasi polinomio $f \in \mathbb{R}[x]$ si possono ottenere a partire dalla fattorizzazione in $\mathbb{C}[x]$, moltiplicando eventuali fattori corrispondenti a radici non reali con il fattore che ha come radice la complessa coniugata, che deve necessariamente comparire nella fattorizzazione in $\mathbb{C}[x]$ di f poiché f ha coefficienti reali. Otteniamo cosi' che la fattorizzazione di f è fatta con polinomi di primo grado o con polinomi di secondo grado e $\Delta < 0$.