Lezione 9 - 3/05/19

martedì 30 aprile 2019 15:09

Def.: Un **ANELLO** è un insieme $(A, +, \cdot)$ tale che
- Gruppo con + Abeliano
- Moltiplicazione Associativa
- Pr. distributive: $a(b+c) = ab+ac \quad (a+b)c = ac+bc$.

Esempi: $\mathbb{R}, \mathbb{Q}, \mathbb{k}[x], A[x] \; \mathbb{k}[x_1, \dots, x_n], \mathbb{k}[[x]] = \{ \sum_{i=0}^{\infty} a_i x^i \mid a_i \in \mathbb{k} \}, \mathrm{Mat}_n(\mathbb{k}), \mathbb{Z}$

Def: Un **IDEALE** $I \subseteq A$ è un sottogruppo di A t.c. $xI \subseteq I \; \forall x \in A$ (cioè vale la propr. di Assorbimento). Indichiamo con $\langle S \rangle$ l'ideale generato da $S \subseteq I$

Oss: È ben definito A/I Anello quoziente: la somma si comporta bene perché I sottogruppo e il prodotto è definito $(x+I)(y+I) = xy+I$. È una buona definizione:
Infatti: $(x+I)(y+I) = xy + xI + yI + I = xy + I$ e inoltre se $x - x' \in I$ e $y - y' \in I$
$(x'+I)(y'+I) = x'y' + I = (x+i)(y+j) + I = xy + I$.

Def: Un **OMOMORFISMO DI ANELLI** è una mappa

$$f: A \longrightarrow B$$

con A e B anelli tale che valga
- $f(x+y) = f(x) + f(y)$
- $f(xy) = f(x) f(y)$

Oss: Deve valere che $f(1) = k$ con k t.c. $k = k^2$:
Infatti $f(1) = f(1 \cdot 1) = f(1) \cdot f(1) = f(1)^2$

Oss: Sia $f: A \longrightarrow B$ di anelli, allora $\ker f$ è ideale di A.
Infatti: Basta verificare l'assorbimento. Sia $a \in \ker f$ allora
$f(ax) = f(a) \cdot f(x) = 0 \cdot f(x) = 0 \quad \forall x \in A$.

I teorema di omomorfismo: Sia $f: A \longrightarrow B$ morfismo di anelli. Allora

$$A/\ker f \simeq \mathrm{Im} f$$

(analogamente $\begin{array}{ccc} A & \xrightarrow{f} & B \\ \downarrow & \circlearrowright & \uparrow \\ A/\ker f & \xrightarrow{\sim} & \mathrm{Im} f \end{array}$)

Dim: Analoga ai gruppi. Si deve solo verificare che $\mathrm{Im} f$ è anello e il resto segue

Def: Sia A un anello. A è un **DOMINIO** se A è commutativo, con unità e vale che $ab = 0 \Rightarrow a = 0 \text{ o } b = 0$

Esempio: $\mathbb{Z}$ è un dominio, $\mathbb{k}[x]$ è un dominio, $\mathbb{Z}_6$ non è un dominio

Fatti:
1. Un dominio finito è un campo
2. A campo $\iff$ $\{0\}$ e A sono gli unici ideali

① Un dominio finito è un campo
② A campo $\iff$ $\{0\}$ e A sono gli unici ideali
① Se A finito $\Rightarrow \exists i,j$ t.c. $x^i = x^j$ $i>j$ $\Rightarrow$ $x^j(x^{i-j}-1)=0$
Se $x\neq 0 \Rightarrow x$ invertibile
② A campo $\iff \forall x\neq 0$ x è invertibile $\iff (x)=(1) \iff \{0\}$ e A sono unici ideali

Def: Un ideale p si dice PRIMO se verifica la seguente proprietà:
Se $xy\in p \Rightarrow x\in p$ o $y\in p$.
Un ideale m si dice MASSIMALE se verifica la seguente proprietà:
Se $m\subseteq J\subseteq A \Rightarrow J=m$ o $J=A$.

Proposizione sacrosanta: Valgono i seguenti fatti:
① $p\subseteq A$ ideale primo $\iff A/p$ è dominio.
② $m\subseteq A$ ideale massimale $\iff A/m$ è campo.

Dim:
① $\Rightarrow$ $(x+p)(y+p)=xy+p\in p \Rightarrow xy\in p$ e (dato che p primo) $x\in p$ o $y\in p$ ✓
$\Leftarrow$ $xy\in p \Rightarrow (x+p)(y+p)\in p \Rightarrow x+p\in p$ o $y+p\in p$ cioè la tesi ✓
② $\Rightarrow$ Sia $x\notin m \Rightarrow (x,m)=1 \Rightarrow ax+\overline{m}=1 \Rightarrow (a+m)(x+m)=1+m$ ✓
$\Leftarrow$ Sia $x+m\neq 0 \Rightarrow (x+m)(a+m)=1 \Rightarrow xa+m=1 \Rightarrow \exists \overline{m}\in m$ t.c. $ax+\overline{m}=1 \Rightarrow$ $(m,x)=1$ cioè m massimale

Corollario sacrosanto: m massimale $\Rightarrow m$ primo
Dim m max $\iff A/m$ campo $\Rightarrow A/m$ dominio $\iff m$ primo

Oss: Il viceversa è falso: Sia $(x)\in \mathbb{K}[x,y] \Rightarrow \mathbb{K}[x,y]/(x) = \mathbb{K}[y]$ dominio, ma NON campo.

Def: Un elemento p si dice PRIMO se $p\mid ab \Rightarrow p\mid a$ o $p\mid b$
Un elemento m si dice IRRIDUCIBILE se $m=ab \Rightarrow a\in A^*$ o $b\in A^*$.

OPERAZIONI TRA IDEALI: Siano I,J ideali di A

① $I\cap J = \{x\in A \mid x\in I, x\in J\}$

② $I+J = \{x+y\in A \mid x\in I, y\in J\}$

③ $IJ = \{xy\in A \mid x\in I, y\in J\}$ **Oss:** $IJ\subseteq I\cap J$ (se $I+J=A \Rightarrow IJ=I\cap J$)
$ij\in I\cap J$ Sia $x\in I\cap J \Rightarrow x\in I$ e $x\in J$
$(i+j)=1$ $(i+j)x=x$
$ix+jx=x \Rightarrow x\in IJ$

④ $I:J = \{x\in A \mid xJ\subseteq I\}$ COLON

⑤ $\sqrt{I} = \{x\in A \mid \exists n\in\mathbb{N}$ t.c. $x^n\in I\}$ **Oss:** • $\sqrt{I}\supseteq I$
• $\sqrt{I}$ è ideale (Lemma $(x+y)^{n+m}$)

Teorema cinese del resto per Anelli: Siano I,J ideali con $I+J=A$. Allora

$$A/IJ \simeq A/I \times A/J$$

Dim: Basta considerare la mappa ovvia e aggregare:

$$\varphi: A \longrightarrow A/I \times A/J, \quad a \longmapsto (a+I,\ a+J)$$

- $\ker\varphi = \{a \mid a\in I, a\in J\} = I\cap J = IJ$.
- φ è surgettiva: Sia $(c+I, d+J)\in A/I \times A/J$. È vero che $\exists a\in A$ t.c.
$$\begin{cases} a+I = c+I \\ a+J = d+J \end{cases} ?$$
considero $i+j=1$ con $i\in I$, $j\in J$. Scelgo $a = id+jc$

Allora $\varphi(id+jc) = (jc+I,\ id+J) = (jc+ic+I,\ id+jd+J) = (c+I, d+J)$ ∎

Fatti Random: Sia $J\supseteq I$ ideali

① J/I è ideale di A/I

Dim: è un sottogruppo per corrispondenza. Devo verificare l'assorbimento:
$(j+I)(x+I) = jx+I \in J+I$.

② $A/J \cong (A/I)/(J/I)$

Dim: Considero la mappa:

$$F: A/I \longrightarrow A/J, \quad a+I \longrightarrow a+J$$

La mappa è ben def perché $J\supseteq I$ e dunque se $a-a'\in I \Rightarrow a-a'\in J$.
Inoltre è banalmente surgettiva ($J\supseteq I$)
$\ker F = \{a+I \mid a\in J\} = J/I$

③ $\sqrt{IJ} = \sqrt{I\cap J} = \sqrt{I}\cap\sqrt{J}$

Dim:
- $IJ\subseteq I\cap J \Rightarrow \sqrt{IJ}\subseteq\sqrt{I\cap J}$
- Sia $x\in\sqrt{I\cap J} \Rightarrow x^n\in I\cap J \Rightarrow x^n\in I$ e $x^n\in J \Rightarrow x\in\sqrt{I}\cap\sqrt{J}$
- Sia $x\in\sqrt{I\cap J} \Rightarrow x^n\in I\cap J \Rightarrow x^n\cdot x^n = x^{2n}\in IJ \Rightarrow x\in\sqrt{IJ}$
- Sia $x\in\sqrt{I}\cap\sqrt{J} \Rightarrow \exists n,m$ t.c. $x^n\in I$, $x^m\in J \Rightarrow x^{n+m}\in IJ \Rightarrow x\in\sqrt{IJ}$.

④ $I+J=A \Rightarrow I^n+J^n=A$

Dim: $i+j=1 \Rightarrow (i+j)^{2n} = 1^{2n}=1$ ma

$$(i+j)^{2n} = \sum_{k=0}^{2n}\binom{2n}{k} i^k j^{2n-k} \in I^n+J^n.$$