Capitolo 4: Teoria degli anelli:

Definizione (Anello):

È un insieme A munito di due operazioni che indicheremo con $+, \cdot$ in modo che:

1- A è un gruppo abeliano rispetto a $+$
2- A è un monoide associativo rispetto al $\cdot$
3- Valgono le leggi distributive delle due operazioni:
   - $\forall\, a, b, c \in A\ a(b + c) = ab + ac$
   - $\forall\, a, b, c \in A\ (a + b)c = ac + bc$

Anello commutativo: Un anello A per il quale la moltiplicazione è commutativa.
Anello con unità: Se esiste un elemento neutro per la moltiplicazione.
Anello di divisione o Corpo: Se gli elementi diversi da 0 formano un gruppo per la moltiplicazione.
Campo: È un corpo commutativo.
Dominio di integrità: Anello commutativo con unità privo di divisori di 0.

Notazione:
Dato un anello A con unità, D sono i divisori di 0 e $A^* = \{x \in A \mid \exists y \in A\,, xy = 1\}$ gli elementi invertibili.

Proprietà importante:
Dato un anello con unità finito $A = A^* \cup D$

Definizione (Sottoanello):

È un sottoinsieme dell'Anello A che con l'operazione da esso indotta è un Anello.

Definizione (Ideale):

Un sottoinsieme I di un Anello A si dice un Ideale se:

1- I è un sottogruppo rispetto a $+$
2- $\forall a \in A\,, \forall x \in I$ vale $ax\,, xa \in I$ (Proprietà di assorbimento)

Esempi interessanti di ideali:
1- Dati I, J ideali allora $(I{:}J) = \{x \in A \mid xJ \subseteq I\}$
2- Dato I ideale $\sqrt{I} = \{x \in A \mid \exists n \in \mathbb{N}\ x^n \in I\}$
3- L'insieme degli elementi nilpotenti è un ideale (Nilradicale)

Definizione (Anello quoziente):

Dato A anello e I un suo ideale possiamo costruire una struttura di anello quoziente $A/_I$ considerando le operazioni:

$$(x + I) + (y + I) = x + y + I$$
$$(x + I) \cdot (y + I) = x \cdot y + I$$

Definizione (Omomorfismo di anelli):

È una funzione tra due anelli A, B |

1. $\forall x, y \in A\, , f(x+y) = f(x) + f(y)$
2. $\forall x, y \in A\, , f(x \cdot y) = f(x) \cdot f(y)$

Esempio:

Omomorfismo di inclusione, Proiezione canonica, Omomorfismo di valutazione.

Proprietà:

$f(0) = 0$

$f(-x) = -f(x)$

Mentre $f(1) = 1$ è assicurato sono le caso in cui B sia un dominio di integrità.

Esempio:

$f: Z_6 \to Z_6\, , f(x) = 3x$ allora $f(1) = 3$

Teorema:

Gli ideali sono tutti e soli i nuclei degli omomorfismi di anelli.

Teorema di omomorfismo per anelli:

Sia $f: A \to B$ un omomorfismo di anelli e $I = \ker(f)$ allora

$\exists!$ omomorfismo di anelli $\varphi: {}^{A}/_{I} \to B \mid f = \varphi \circ \pi$

Inoltre φ è iniettivo. φ è surgettivo $\leftrightarrow$ f è surgettivo.

Definizione (Caratteristica):

$\mathrm{char}(A) = \min_{\mathbb{N}} m \mid \forall x \in A\, , mx = 0$

Osservazione:

Se $\nexists m$ con questa proprietà $\mathrm{char}(A) = 0$

Attenzioni:
Le proprietà seguenti sono relative ad anelli commutativi con unità.

Proposizione:
Sia A anello commutativo con unità, allora:
$$\mathrm{char}(A) = \begin{cases} \mathrm{ord}(1) \text{ se} < \infty \\ 0 \text{ se} = \infty \end{cases}$$
Dove $\mathrm{ord}(1)$ è l'ordine di 1 per l'operazione di somma.

Proposizione:
Sia A un anello commutativo con unità.
$\mathrm{char}(A) = m \to A$ contiene un sottoanello isomorfo a $Z/_{mZ}$
$\mathrm{char}(A) = 0 \to A$ contiene un sottoanello isomorfo a Z

Notazione:
Il sottoanello di A così costruito si chiama **sottoanello fondamentale**.

Proposizione (Intersezione fra ideali):
Sia A anello commutativo con unità, I, J ideali di A. Allora $I \cap J$ è un ideale di A.

<u>Definizione (Ideale somma):</u>
$I + J = \{x + y \mid x \in I, y \in J\}$ è il più piccolo ideale contente I e J.

Osservazione:
Se abbiamo osservato che $A = I + J \to \forall\, i \in I, \forall\, j \in J\ \exists x, y \in A \mid xi + yj = 1$

<u>Definizione (Ideale prodotto):</u>
$IJ = \{x_1 y_1 + \dots + x_n y_n \mid x_i \in I, y_i \in J\ , n > 0\}$

Esempio:
$A = \mathbb{Z}\ , I = (m), J = (n), IJ = (m \cdot n)\ , I \cup J = ([m,n])\ , I + J = \big((m,n)\big)$

Osservazione:
$IJ \subseteq I \cap J$

<u>Definizione (Ideale proprio):</u>
Un ideale I di A si dice proprio se $I \neq A$.

Osservazione:
Un ideale è proprio $\leftrightarrow 1 \notin I \leftrightarrow I \cap A^* = \emptyset$
Sia $x \in A$, $\exists$ un ideale proprio contenente $x \leftrightarrow x \notin A^*$

<u>Proposizione (Caratterizzazione campo):</u>

Gli unici ideali di un anello commutativo con unità sono $\{0\}$ e $A \leftrightarrow A$ è un campo.

<u>Definizione (Massimale):</u>

Un ideale proprio M di A commutativo con unità si dice massimale se, dato I ideale di A si ha che: $M \subseteq I \subseteq A \rightarrow I = M$ oppure $I = A$.

Proposizione:

Sia A commutativo con unità e $x \in A$ non invertibile $\rightarrow \exists$ un ideale mass. contenente x.

<u>Definizione (Ideale primo):</u>

Un ideale proprio P di un anello A commutativo con unità si dice primo se:
$xy \in P \rightarrow x \in P$ oppure $y \in P$.

Proprietà:

Un ideale principale è primo $\leftrightarrow$ è generato da un elemento primo.
π proiezione, P ideale primo allora $\pi^{-1}(P)$ è un ideale primo contenente $\ker \pi$
$A/_P$ è un dominio di integrità $\leftrightarrow$ P ideale primo
$A/_M$ è un campo $\leftrightarrow$ M ideale massimale
Massimale $\rightarrow$ Primo

<u>Teorema cinese per anelli:</u>

Siano I, J due ideali di $A \mid I + J = A$ allora: $A/_{I \cap J} \cong A/_I \times A/_J$

Proposizione:

Siano I, J due ideali di $A \mid I + J = A$ (Si dicono **coprimi**) allora: $I \cap J = IJ$

Approfondimento:

Come $\mathbb{Z}$ (Dom. di integrità) viene esteso a $\mathbb{Q}$ per risolvere le equazioni a coefficienti interi del tipo $ax = b$.

Dato A dominio di integrità e sia $S \subseteq A$ |

1. $0 \notin S$
2. $1 \in S$
3. S è moltiplicativamente chiuso, $s, t \in S \rightarrow s \cdot t \in S$

Allora $S^{-1}A := \left\{\frac{a}{s} \mid a \in A, s \in S\right\}/\sim$ con $\frac{a}{b} \sim \frac{c}{d} \leftrightarrow ad = cb$

Con operazioni di somma e prodotto definite come:
$\frac{a}{s} + \frac{b}{t} = \frac{at+bs}{st}$; $\frac{a}{s} \cdot \frac{b}{t} = \frac{ab}{st}$

Proposizione:

La funzione $f: A \rightarrow S^{-1}A \mid f(x) = \frac{x}{1}\ \forall x \in A$ è un omomorfismo iniettivo.

Esempio:
$S^{-1}\mathbb{Z} = \left\{\frac{a}{2^n} \mid a \in \mathbb{Z}, n \in \mathbb{N}\right\}$; $S = \{2^n, n \in \mathbb{N}\}$

Proposizione:

$S^{-1}I$ è un ideale di $S^{-1}A$

Proposizione:

Se J è un ideale di $S^{-1}A$ allora $J = S^{-1}I$ per un ideale I di A.

Attenzione:
Non è biunivoca, ci sono ideali propri di A che corrispondono ad ideali banali di $S^{-1}A$.

Osservazione:
$S^{-1}I = S^{-1}A \leftrightarrow I \cap S \neq \emptyset$

Esempi ed esercizi:

Gli esercizi più standard riguardano piccole dimostrazioni sulle radici dei polinomi e il procedimento inverso, dato un elemento individuare il polinomio minimo per cui sia una radice.
Quelli meno standard sono prevalentemente dimostrazioni sugli ideali.

Esempio 1:
Sia $\alpha \in \mathbb{C}$ una radice di $x^3 + 2x - 1$.
Trovare il polinomio minimo di $\alpha + 1$; α^{-1} ; $\alpha^2 + 1$ su $\mathbb{Q}$

Studiamo l'equazione data e cerchiamo di vedere se è fattorizzabile in $\mathbb{Q}$. Essendo irriducibile per verifica diretta sulle radici in $\mathbb{Q}$ ricaviamo che $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$.
Questo passaggio è importante per sapere la dimensione del polinomio che sto cercando.
Sfruttiamo quindi la condizione dettata dall'equazione, $\alpha^3 + 2\alpha - 1 = 0$:

$(\alpha - 1) \to g(x) = f(x-1)$ quindi il p.m. è: $(x-1)^3 + 2(x-1) - 1$
$(\alpha^2 + 1)$ in questo caso non risulta evidente, costruiamo quindi il sistema lineare dato dall'equazione:
$(\alpha^2+1)^3 + a(\alpha^2+1)^2 + b(\alpha^2+1) + c = 0$; sfruttando l'equazione iniziale calcoliamo le potenze:
$(\alpha^2+1)^3 = \alpha^2 - \alpha + 2$; $(\alpha^2+1)^2 = \alpha + 1$ il sistema diventa dunque:
$(1+a)\alpha^2 + (-1+b)\alpha + (2+a+b+c) = 0$ lo uguagliamo a quello iniziale e troviamo il polinomio minimo: $g(x) = x^3 - 2x^2 - 1$

$(\alpha^{-1}) \to$ osserviamo che per calcolare un inversa possiamo sfruttare il **polinomio reciproco** (Ossia quello calcolato invertendo l'ordine dei coefficienti), quindi $g(x) = -x^3 + 2x + 1$

Esempio 2:
Determinare il polinomio minimo di $\sqrt{2\sqrt{2} - 3}$ su $\mathbb{Q}$.

Si procede cercando per prima cosa un polinomio che si annulli su quella radice, da quello estraiamo poi il polinomio minimo.
Eliminiamo una radice o un fattore dopo l'altro:

$$x^2 = 2\sqrt{2} - 3 \to x^2 + 3 = 2\sqrt{2} \to (x^2+3)^2 = 8 \to x^4 + 6x^2 + 1 = 0$$

Dimostrandone l'irriducibilità abbiamo concluso.