Lezione del 1 aprile; Registro dettagliato

Il parallelismo fra la teoria che parte dal teorema sulla divisione con resto e porta al teorema di fattorizzazione unica nell'anello $\mathbb{Z}$ degli interi e negli anelli $\mathbb{K}[x]$ di polinomi a coefficienti in un campo $\mathbb{K}$ suggerisce la definizione di un certo tipo di anelli, gli anelli, o domini, euclidei. Storicamente, la teoria dei domini euclidei emerge dallo sviluppo della teoria dell'anello $\mathbb{Z}[i]$ degli interi Gaussiani e di altri domini di interi algebrici, sotto l'impulso di problemi di teoria dei numeri.

In questa lezione, dopo avere introdotto la terminologia sulle questioni di divisibilita' in un dominio di integrita', diamo la definizione di dominio euclideo, enunciamo che un tale dominio e' ad ideali principali (omettendo la dimostrazione, analoga a quella in $\mathbb{Z}$), da cio' deduciamo che in esso vale l'identita' di Bezout (in forma debole), da questa deduciamo l'analogo del lemma di Euclide, ed enunciamo il teorema di fattorizzazione unica (omettendo la dimostrazione, analoga a quella in $\mathbb{Z}$).

1.X- Divisibilita' in un dominio di integrita'.

1.1- Relazione di preordine "divide", e relative relazioni d'equivalenza e d'ordine parziale.

1.2- Corrispondenza fra elementi ed ideali principali, dualita' rispetto alle relazioni "divide" ed "e' contenuto".

1.3- Elementi irriducibili; elementi primi.

2.X- Domini euclidei.

2.1- Definizione.

2.2- Th. Un dominio euclieo e' ad ideali principali.

Th. Identita' di Bezout.

2.3- Lemma. Irriducibile implica primo.

Th. di fattorizzaione unica.

1.X- Divisibilita' in un dominio di integrita'. Di seguito fino ad avviso contrario A denota un dominio d'integrita'. Al posto di dire che un elemento e' invertibile nell'anello diremo spesso che e' una unita' dell'anello, ed indicheremo con A^* il gruppo delle unita' di A.

1.1- Relazione di preordine "divide", e relative relazioni d'equivalenza e d'ordine parziale.

Per ogni $a, b \in A$ si dice che a divide b e si scrive $a|b$ se e solo se esiste un $c \in A$ tale che $ac = b$. In particolare, per ogni $a \in A$ si ha che $1|a$ ed $a|0$. La relazione "divide" e' una relazione di preordine su A. Per ogni $a, b \in A$ si dice che a e' associato a b e si scrive $a \sim b$ se e solo se $a|b$ e $b|a$; cio' capita se e solo se esiste un $c \in A^*$ tale che $ac = b$. Sull'insieme quoziente $A/\sim$ la relazione "divide" induce una relazione d'ordine parziale. (Queste costruzioni e fatti si hanno in generale per ogni relazione di preordine).

Due elementi $a, b \in A$ diversi da 0 e non unita' si dicono coprimi se e solo se gli unici divisori comuni di a e b sono le unita'.

1.2- Corrispondenza fra elementi ed ideali principali, dualita' rispetto alle relazioni "divide" ed "e' contenuto".

L'ideale di A generato da $a_1, \ldots, a_p \in A$ si indica con $(a_1, \ldots, a_p)$; questo ideale e' dato esplicitamente da $(a_1, \ldots, a_p) = \{a_1x_1 + \cdots + a_px_p |\ x_1, \ldots, x_p \in A\}$. Un ideale generabile da un solo elemento si dice ideale principale.

Si hanno i seguenti fatti:

- $(a) = \{0\}$ sse $a = 0$ e $(a) = A$ sse $a \in A^*$;

- $a|b$ sse $(a) \ni b$ sse $(a) \supseteq (b)$;

- $a \sim b$ sse $(a) = (b)$.

Da cio' segue che la funzione

$$A/\sim \to \mathcal{IP}(A), \quad a \mapsto (a)$$

dall'insieme $A/\sim$ quoziente di A rispetto alla relazione $\sim$ ordinato rispetto alla relazione indotta da $|$ all'insieme $\mathcal{IP}(A)$ degli ideali principlai di A ordinato rispetto all'inclusione insiemistica, e' una dualita' di insiemi parzialmente ordinati.

1.3- Elementi irriducibili; elementi primi.

Definizione. Un elemento di A diverso da 0 si dice irriducibile se e solo se non e' un'unita' e non si puo' scrivere come prodotto di due non unita' o, equivalentemente, se e solo se non e' un'unita' ed e' diviso solo dalle unita' e dai suoi associati. La condizione $\neq 0$ in realta' e' implicata dalle altre, ma si mette per chiarezza. In termini di ideali si ha: a e' irriducibile se e solo se $(a) \subset A$ e $(a) \subset (c)$ solo per $(c) = A$ ($\subset$ indica inclusione propria).

Definizione. Un elemento di A diverso da 0 si dice primo se e solo se non e' un'unita' ed ogniqualvolta divide un prodotto divide anche almeno uno dei fattori.

Segue direttamente dalle definizioni che gni elemento primo e' anche irriducibile.

2.X- Domini euclidei.

2.1- **Definizione.** Un dominio d'integrita' A si dice dominio euclideo se e solo se esiste una funzione $\nu : (A \setminus \{0\}) \to \mathbb{N}$ tale che

per ogni a, b non zero in A, $\nu(a) \leq \nu(ab)$;

per ogni $a, b \in A$ con $b \neq 0$, esistono $q, r \in A$ tali che

$$a = qb + r, \quad \text{con} \quad \nu(r) < \nu(b) \ \text{ oppure } r = 0.$$

Gli elementi q ed r si dicono rispettivamente quoziente e resto della divisione di a su b. Si noti che non si chiede l'unicita'.

2.2- **Teorema**. Un dominio euclieo e' ad ideali principali. (Si dimostra come in $\mathbb{Z}$.)

Teorema (Identita' di Bezout, debole). Due elementi a, b non 0 e non unita' in un dominio euclideo A sono coprimi se e solo se esistono $x, y \in A$ tali che

$$ax + by = 1.$$

Dimostrazione.

Parte "se". Se esistono $x, y \in A$ tali che $ax + by = 1$, allora ogni divisore comune di a, b deve essere anche un divisore di 1, e quindi deve essere una unita'.

Parte "solo se". Se a e b sono coprimi, allora l'unico ideale principale di A contenente sia (a) che (b) e' A. Ora, (a, b) e' un ideale contenente sia (a) che (b) ed e' principale, perche' tutti gli ideali di A sono principali. Dunque $(a, b) = A$, in particolare $(a, b) \ni 1$, ed esistono $x, y \in A$ tali che $ax + by = 1$.

2.3- **Lemma (di Euclide/Gauss).** In un dominio euclideo ogni elemento irriducibile e' primo.

Dimostrazione. Siano p, a, b elementi in un dominio euclideo, con p irriducibile che divide ab ma non divide a; proviamo che p divide b.

Si ha $a, b \neq 0$. Se a e' una unita' allora p divide b. Se a non e' un'unita', allora p e a sono coprimi (essendo p irriducibile e $p \not| a$) e per l'identita' di Bezout si ha che esistono $x, y \in A$ tali che $px + ay = 1$; moltiplicando entrambe i membri per b si ha $pbx + aby = b$. Ora, $ab = pq$ per qualche $q \in A$ (poiche' $p|ab$) e dunque

$$b = pbx + pqy = p(bx + qy),$$

cioe' $p|b$.

Teorema di unica fattorizzazione. In un dominio euclideo ciascun elemento non nullo e non unita' si puo' scrivere come prodotto di (un numero finito di) elementi irriducibili; ogni due scritture di uno stesso elemento hanno lo stesso numero di fattori e si possono riordinare in modo che fattori corrispondenti siano associati. (Si dimostra come in $\mathbb{Z}$)