UNIVERSITÀ DEGLI STUDI ROMA TRE
Corso di Laurea in Matematica
AL2 - Algebra 2 - Gruppi, Anelli e Campi - A.A. 2008/2009

Test di autovalutazione sugli anelli

Definizione. $(R, +, \cdot)$ è un anello se:
- $(R, +)$ è un gruppo abeliano;
- il prodotto è associativo;
- valgono le leggi distributive.

Un anello R è :
- UNITARIO se possiede l'elemento neutro rispetto al prodotto (l'unità);
- COMMUTATIVO se il prodotto è commutativo;
- INTEGRO se non possiede divisori dello zero, cioè $ab = 0 \Rightarrow a = 0$ e/o $b = 0$;
- un DOMINIO se è unitario, commutativo e integro.
- un CORPO se è unitario ed ogni elemento non zero è invertibile rispetto al prodotto;
- un CAMPO se è unitario, commutativo ed ogni elemento non zero è invertibile rispetto al prodotto (cioè $(R*, \cdot)$ è un geruppo abeliano).

Osserviamo che se ogni elemento non zero è invertibile rispetto al prodotto allora l'anello è integro, infatti se $ab = 0$ e $a \neq 0$, $b \neq 0$, allora $b = a^{-1}ab = a^{-1}0 = 0$ contro l'ipotesi che $b \neq 0$.

Sottoanelli. Dato un anello $(R, +, \cdot)$ ed un suo sottoinsieme S, allora S è un SOTTOANELLO di R se S è un anello rispetto alle stesse operazioni di R.

Attenzione: Alcune proprietà di un anello si trasferiscono sempre ai suoi sottoanelli (se R è commutativo o integro anche S lo sarà). Però altre non si trasferiscono necessariamente. Ad esempio se R è unitario non è detto che S lo sia, così come l'invertibilità degli elementi non zero (basta prendere $\mathbb{Z} \subset \mathbb{Q}$).

Rispondere alle seguenti domande:
- Sottoanello generato da un un insieme di elementi X.
- Condizioni necessarie e sufficienti affinché un sottoinsieme sia un sottoanello.

Ideali.

Dato un anello $(R, +, \cdot)$ ed un suo sottoinsieme I, allora I è un IDEALE dx, sx, bil, di R se $(I, +)$ è un gruppo abeliano e per ogni $x \in R$, $i \in I$ si ha che $ix \in I$, $xi \in R$ o entrambe.

Rispondere alle seguenti domande:

- Differenza fra sottoanello e ideale.
- Ideale generato da un sottoinsieme X. Differenza fra il caso unitario e quello non unitario.
- L'intersezione di ideali è un ideale? E l'unione? E la somma?
- Relazione di equivalenza compatibile su un anello: definizione. A cosa serve? Una relazione compatibile è sempre associata ad un ideale bilatero: in quale modo?
- Viceversa, dato un ideale bilatero I, possiamo associare ad I una relazione compatibile? Cosa vuol dire quozientare un anello rispetto ad un ideale? Come si applica questo discorso al caso $\mathbb{Z}_n$?
- Definire un ideale primo e un ideale massimale. Come si possono caratterizzare tali ideali utilizzando i quozienti di R? C'è differenza fra il caso unitario e non?
- Sussite qualche relazione fra ideale primo e massimale? C'è differenza fra il caso unitario e non?
- Esistono sempre gli ideali massimali in un anello?

Omomorfismi di anelli.

Data un'applicazione fra anelli $\varphi : (A, +, \cdot) \to (B, +, \cdot)$, diciamo che φ è un omomorfismo se $\varphi(a + b) = \varphi(a) + \varphi(b)$ e $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$.

Rispondere alle seguenti domande:

- φ è anche un omomorfismo di gruppi?
- $\varphi(0)$ è sempre 0 o può assumere anche altri valori? Se la risposta è NO, fornire un controesempio.
- Se gli anelli sono unitari, $\varphi(1)$ è sempre 1 o pu assumere anche altri valori? Se la risposta è NO, fornire un controesempio.
- Come si identificano gli elementi che hanno la stessa immagine?
- Quando un omomorfismo è iniettivo?
- Come si corrispondono ideali e sottoanelli di A e B tramite φ?
- E gli ideali primi e massimali restano tali tramite φ e φ^{-1}? Se la risposta è NO, fornire un controesempio.
- Enunciare e dimostrare il Teorema di Omomorfismo.

- Applicazioni del Teorema: i due Teoremi di Isomorfismo, la caratteristica di un anello unitario.

Campo dei quozienti di un anello.

DA INSERIRE

Divisibilità nei domini.

Sia A un dominio. Rispondere alle seguenti domande:

- Che tipo di relazione è quella di divisibilità ($a \mid b$ se e solo se $b = bh$, esiste $h \in \mathbb{Z}$)? E quella di "essere associati" per due elementi di A?
- Dare la definizione di elemento irriducibile e di elemento primo.
- Che relazione intercorre fra queste due nozioni?
- Definire il MCD fra due elementi di A. Esso è unico? Può essere definito per due qualsiasi elementi di A?
- Come si può descrivere il MCD a livello di ideali?
- Cos'è l'Identità di Bezout? Essa è unica? Esiste sempre? Come può essere interpretata a livello di ideali?
- Può esistere il MCD senza l'Identità di Bezout? E l'Identità di Bezout senza il MCD?
- Come si definisce un UFD?
- Cos'è la condizione della catena ascendente sugli ideali principali?
- Come si può utilizzare la condizione della catena ascendente sugli ideali principali per caratterizzare gli UFD?
- Un UFD è sempre un MCD-dominio? E un UFD è sempre un dominio di Bezout?
- Cos'è un dominio a Ideali Principali (PID)?
- Come sono fatti gli ideali primi e gli ideali massimali in un PID?
- Quali proprietà di divisibilità verifica un PID?
- Esempi di UFD che non sono PID.
- Quando un anello di polinomio $A[X]$ è un PID?
- Cos'è un dominio Euclideo (ED)? Darne alcuni esempi.
- Come si può fare la divisione euclidea in $\mathbb{Z}[i]$?
- Un ED è un PID? E un PID è un ED? Se la risposta è negativa dare un controesempio.
- Quali fra le seguenti proprietà si trasferiscono da un dominio A ad $A[X]$? UFD, PID, ED, Bezout. Quando la risposta è positiva fornire una dimostrazione, quando è negativa fornire un controesempio.

- Polinomi primitivi e loro prodotti.
- Polinomi irriducibili in $A[X]$ ed in $K[X]$, essendo K il campo dei quozienti di A. Passaggio dell'irriducibilità da $A[X]$ a $K[X]$ e viceversa, quando A è un dominio con il MCD.

Campi.

- Cos'è un ampliamento di campi?
- Quanti elementi ha un campo finito?
- Cos'è il grado di un'estensione di campi?
- Quanti elementi ha un campo finito?
- Come si costruisce un campo finito?
- Sia K un campo. Quali sono gli elementi invertibili di $K[X]/I$, dove I è un ideale di $K[X]$?
- Come si possono descrivere tutti gli elementi di $K[X]/I$?