ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

Anno Accademico *2010/2011*

Facoltà *Scienze Matematiche, Fisiche e Naturali*

Corsi di Laurea o di Diploma *Triennale in Matematica*

Insegnamento **Algebra I**

Docente titolare del corso prof. Mirella Manaresi

Altri docenti partecipanti (modulo)

Data inizio Lezioni 5 ottobre 2010

Data fine Lezioni 20 dicembre 2010

Da consegnare al docente tramite la Presidenza della Facoltà di appartenenza entro il 31 ottobre e da riconsegnare improrogabilmente al Preside della medesima Facoltà entro 15 gg. dal termine delle lezioni.

Luogo (Aula) ***Aula Cremona***

Data ***5 ottobre 2010***

Introduzione al corso: obiettivi, modalitá d'esame, ricevimento studenti, informazioni varie.
Brevi richiami di teoria degli insiemi: insieme delle parti di un insieme, intersezioni e unioni di insiemi, ricoprimenti e partizioni di un insieme, complementare di un sottoinsieme rispetto a un insieme dato, prodotto cartesiano di due insiemi, applicazioni tra insiemi. Applicazioni iniettive e applicazioni suriettive.

Ore 2 (9-11) ***Firma (Mirella Manaresi)***

Luogo (Aula) ***Aula Cremona***

Data ***6 ottobre 2010***

Applicazioni biunivoche. Immagine di un sottoinsieme del dominio mediante un'applicazione; controimmagine di un punto e di un sottoinsieme del codominio mediante un'applicazione. Restrizione di un'applicazione. Composizione di applicazioni e sue proprietá, diagrammi commutativi. Applicazione inversa di un'applicazione biunivoca. Applicazioni tra insiemi finiti.

Ore 2 (11-13) ***Firma (Mirella Manaresi)***

Luogo (Aula) ***Aula Tonelli***

Data ***7 ottobre 2010***

Relazioni tra insiemi. Proprietá di una relazione su un insieme. Relazioni di equivalenza. Classi di equivalenza rispetto ad una relazione di equivalenza, insieme quoziente. Esempi ed esercizi.

Ore 2 (9-11) ***Firma (Mirella Manaresi)***

Luogo (Aula) ***Aula Cremona***

Data ***12 ottobre 2010***

Relazione di equivalenza associata ad una partizione. Relazione di equivalenza R_f su X associata ad una applicazione f da X ad Y. Passaggio al quoziente di un'applicazione f da X ad Y rispetto ad una relazione di equivalenza definita su X. Esercizi sugli insiemi quoziente.
Relazioni di ordine e relazioni di ordine totale. Esempi.

Ore 2 (9-11) ***Firma (Mirella Manaresi)***

Luogo (Aula) ***Aula Cremona***

Data ***13 ottobre 2010***

Buon ordinamento. Esercizi sulle relazioni d'ordine. Minimo di un sottoinsieme di Z. Esempi. Principio del minimo. Principio di induzione matematica. Esempi di applicazione del principio di induzione. Esercizi. Coefficienti binomiali $\binom{n}{k}$ e loro proprietá. I coefficienti binomiali sono interi.

Ore 2 (9-11) ***Firma (Mirella Manaresi)***

Luogo (Aula) ***Aula Tonelli***

Data ***14 ottobre 2010***

Teorema del binomio. Il numero dei sottoinsiemi con k elementi di un insieme con n elementi é $\binom{n}{k}$. Divisibilitá tra interi e sue proprietá. Numeri primi. Fattorizzazione di un intero positivo in un prodotto di primi. Esistenza di infiniti primi.

Ore 2 (9-11) ***Firma (Mirella Manaresi)***

Luogo (Aula) ***Aula Cremona***

Data ***19 ottobre 2010***

Massimo comun divisore di due interi. Lemma di divisione. Esistenza del massimo comun divisore e sua espressione come combinazione lineare dei due interi. Alcune conseguenze dell'esistenza del massimo comun divisore e della sua espressione come combinazione dei due interi. Teorema Fondamentale dell'Aritmetica. L'algoritmo euclideo per la determinazione del massimo comun divisore di due interi.

Ore 2 (9-11) ***Firma (Mirella Manaresi)***

Luogo (Aula) ***Aula Cremona***

Data ***20 ottobre 2010***

Calcolo del massimo comun divisore attraverso l'algoritmo euclideo. L'equazione diofantea $ax+by = c$ con a, b, c interi. Esercizi su massimo comun divisore ed equazioni diofantee. Alcune note storiche sui numeri primi: crivello di Eratostene, congettura di Gauss, Teorema dei numeri primi, congettura di Golbach, congettura dei primi gemelli. Congruenze modulo m: definizione di interi congruenti, relazione di congruenza e sue proprietá. Due interi sono congruenti modulo m se e solo se hanno lo stesso resto modulo m.

Ore 2 (9-11) ***Firma (Mirella Manaresi)***

Luogo (Aula) ***Aula Tonelli***

Data ***21 ottobre 2010***

Comportamento della relazione di congruenza rispetto a somma, prodotto e potenze. Piccolo teorema di Fermat. Seconda formulazione del piccolo teorema di Fermat; equivalenza delle due formulazioni. Enunciato del teorema di Eulero.
Criteri di divisibilitá per $3, 4, 5, 9, 11$.
Classi di congruenza modulo m*, l'insieme quoziente* Z_m.

Ore 2 (9-11) ***Firma (Mirella Manaresi)***

Luogo (Aula) ***Aula Cremona***

Data ***26 ottobre 2010***

Operazioni di somma e prodotto fra classi di congruenza modulo m *e loro proprietá. Caratterizzazione degli elementi invertibili rispetto al prodotto. Esempi.*
La congruenza $ax \equiv b \pmod{m}$ *con* $a, b \in Z$ *ammette soluzioni intere se e solo se* $d = M.C.D.(a, m)$ *divide* b*. Se ci sono soluzioni queste si distribuiscono esattamente in* d *classi di congruenza modulo* m*. Esempi.*
Esercizi su divisibilitá, classi di congruenza, elementi invertibili di Z_m*, congruenze.*

Ore 4 (9-13) ***Firma (Mirella Manaresi)***

Luogo (Aula) ***Aula Cremona***

Data ***27 ottobre 2010***

Teorema cinese dei resti. Esempi. Condizione necessaria e sufficiente affinche' un sistema di congruenze abbia soluzioni. Esempi.
Esercizi su divisibilitá tra interi, elementi invertibili di Z_m*, congruenze, sistemi di congruenze.*

Ore 2 (9-11) ***Firma (Mirella Manaresi)***

Luogo (Aula) ***Aula Tonelli***

Data ***28 ottobre 2010***

Definizione di semigruppo, monoide, gruppo. Esempi. Unicitá dell'elemento neutro di un monoide; potenze (risp. multipli) con esponente naturale degli elementi di un monoide. In un gruppo vale la legge di cancellazione e l'inverso di ogni elemento é unico. Potenze (risp. multipli) con esponente intero degli elementi di un gruppo.
Ordine (o periodo) di un elemento di un gruppo. Esempi. Se l'ordine di $a \in G$ *é uguale ad* m*, allora* $a^k = e_G$ *se e solo se* m *divide* k*. Un elemento di un gruppo finito ha sempre ordine finito.*
Gruppo prodotto diretto di due gruppi dati. Esempi.

Ore 2 (9-11) ***Firma (Mirella Manaresi)***

Luogo (Aula) ***Aula Cremona***

Data ***3 novembre 2010***

Calcolo dell'ordine di elementi di gruppi, in particolare calcolo dell'ordine di $[a]_m$ nel gruppo $(Z_m, +)$ e calcolo dell'ordine di elementi di gruppi prodotto diretto.
Sottogruppi: definizione ed esempi. Sottogruppo generato da un elemento. Sottogruppi di $(Z, +)$. Il sottogruppo generato da un elemento é sempre abeliano e ha tanti elementi quanto é l'ordine del generatore. Esempi. Gruppi ciclici. Esempi di gruppi ciclici: Z, Z_m con $m > 1$, $Z_m \times Z_n$ con m e n primi tra loro. $Z_m \times Z_m$ non é ciclico.
L'insieme $S(X)$ delle biezioni su un insieme non vuoto X con l'operazione di composizione é un gruppo. Se X é finito e ha n elementi, allora $S(X)$ ha $n!$ elementi.

Ore 2 (9-11) ***Firma (Mirella Manaresi)***

Luogo (Aula) ***Aula Tonelli***

Data ***4 novembre 2010***

Se $X = 1, 2, ..., n$, $S(X)$, denotato con S_n, é detto gruppo simmetrico su n lettere e ha $n!$ elementi. Composizione di due permutazioni, inversa di una permutazione. Cicli. Ordine di un ciclo. Studio del gruppo simmetrico per $n = 3$: descrizione degli elementi, costruzione della tavola di moltiplicazione. Due cicli disgiunti commutano. Orbite di una permutazione. Ogni permutazione diversa dall'identitá é prodotto in modo unico di cicli disgiunti.

Ore 2 (9-11) ***Firma (Mirella Manaresi)***

Luogo (Aula) ***Aula Cremona***

Data ***9 novembre 2010***

Dimostrazione del teorema di decomposizione. Esempi. Ordine di una permutazione. Trasposizioni. Se una permutazione si scrive come prodotto di r trasposizioni e di s trasposizioni, allora r ed s sono congrui modulo 2. Segno di una permutazione e sue proprietá. Permutazioni pari e permutazioni dispari. Gruppo alterno su n lettere. Il gruppo A_n ha $\frac{n!}{2}$ elementi. Esempi ed esercizi.

Ore 2 (9-11) ***Firma (Mirella Manaresi)***

Luogo (Aula) ***Aula Cremona***

Data ***10 novembre 2010***

L'intersezione di sottogruppi é un sottogruppo. L'unione insiemistica di sottogruppi non é un sottogruppo. Sottogruppo generato da un sottoinsieme di un gruppo. Sottogruppo generato da un numero finito di elementi che commutano tra loro. Esempi. Ogni sottogruppo di un gruppo ciclico é un gruppo ciclico. Il gruppo $(Q, +)$ non é ciclico. Esercizi.

Ore 2 (9-11) ***Firma (Mirella Manaresi)***

Luogo (Aula) ***Aula Tonelli***

Data ***11 novembre 2010***

Sottogruppi di Z_m: per ogni d che divide m esiste uno e un solo sottogruppo di Z_m con d elementi. Sottogruppi di un gruppo prodotto diretto: il prodotto di sottogruppi é un sottogruppo del prodotto, ma non tutti i sottogruppi del prodotto sono prodotti di sottogruppi. Esempi ed esercizi. Un gruppo infinito ha infiniti sottogruppi distinti.
Esercizi sui sottogruppi di S_n.

Ore 2 (9-11) ***Firma (Mirella Manaresi)***

Luogo (Aula) ***Aula Cremona***

Data ***16 novembre 2010***

Relazioni di equivalenza modulo un sottogruppo. Laterali destri e laterali sinistri di un sottogruppo H in un gruppo G. Corrispondenza biunivoca tra H e un suo qualunque laterale destro (sinistro). Corrispondenza biunivoca tra l'insieme dei laterali destri e dei laterali sinistri di un sottogruppo. Esempi ed esercizi.
Teorema di Lagrange e alcuni suoi corollari. i gruppi di ordine primo sono ciclici. I gruppi di ordine minore di 6 sono tutti abeliani. Gruppi di ordine 4 non ciclici. Esercizi. Omomorfismi di gruppi; definizione e prime proprietá. Esempi. Nucleo e immagine di un omomorfismo di gruppi. Esempi.

Ore 4 (9-13) ***Firma (Mirella Manaresi)***

Luogo (Aula) ***Aula Cremona***

Data ***17 novembre 2010***

L'immagine di un sottogruppo in un omomorfismo di gruppi é un sottogruppo, la controimmagine di un sottogruppo é un sottogruppo. Se due elementi commutano, allora commutano anche le loro immagini mediante un omomorfismo. Se $\phi : G \to H$ é un omomorfismo di gruppi e $g \in G$ é un elemento di periodo m, allora il periodo di $\phi(g)$ divide m. L'immagine omomorfa di un gruppo ciclico é un gruppo ciclico. Un omomorfismo di gruppi da un gruppo ciclico G ad un gruppo H é determinato dall'immagine di un generatore di G. Omomorfismi da Z ad un gruppo G. Omomorfismi da Z_m ad un gruppo G, in particolare omomorfismi da Z_m a Z_n e da Z_m a S_n.
Un omomorfismo di gruppi $\phi : G \to H$ é iniettivo se e solo se il suo nucleo é $\{e_G\}$.

Ore 2 (9-11) ***Firma (Mirella Manaresi)***

Luogo (Aula) ***Aula Tonelli***

Data ***18 novembre 2010***

Isomorfismi di gruppi. L'applicazione inversa di un isomorfismo di gruppi é un omomorfismo di gruppi. La relazione di isomorfismo é una relazione di equivalenza nella famiglia di tutti i gruppi. Proprietá che si conservano per isomorfismo. Esempi.
Struttura di gruppo sull'insieme quoziente G/R_ϕ dove G é un gruppo e $\phi : G \to H$ é un omomorfismo di gruppi. In questo caso la relazione R_ϕ coincide con la relazione di equivalenza $\equiv_{\ker(\phi)}$ modulo il sottogruppo $\ker(\phi)$. Teorema fondamentale di isomorfismo per gruppi. Ogni gruppo ciclico infinito é isomorfo a Z.

Ore 2 (9-11) ***Firma (Mirella Manaresi)***

Luogo (Aula) ***Aula Cremona***

Data ***23 novembre 2010***

Ogni gruppo ciclico di ordine m é isomorfo a Z_m .
Anelli unitari: definizioni ed esempi. Unicitá dell'unitá di un anello. Formula del binomio e differenza di due potenze n-esime in un anello commutativo. Sottoanelli. Divisori dello zero. Domini d'integritá. Un sottoanello di un dominio di integritá é un dominio d'integritá. Divisori dello zero in Z_m; se m é primo Z_m é un dominio di integritá. L'anello prodotto diretto $Z \times Z$ non é un dominio d'integritá.

Ore 2 (9-11) ***Firma (Mirella Manaresi)***

Luogo (Aula) ***Aula Cremona***

Data ***24 novembre 2010***

Risoluzione di un esercizio di una prova d'esame.
Elementi invertibili di un anello. Un elemento invertibile non é uno zero-divisore, ma un non zero divisore puó non essere invertibile. Esempi. Campi.
Ideali di un anello commutativo unitario. Ideali propri. Esempi. Un ideale é tutto l'anello se e solo se contiene un elemento invertibile. L'ideale generato da un elemento e il sottogruppo generato dall'elemento. Ideale generato da un numero finito di elementi. Un anello é un campo se e solo se i suoi unici ideali sono quelli banali.

Ore 2 (9-11) ***Firma (Mirella Manaresi)***

Luogo (Aula) ***Aula Tonelli***

Data ***25 novembre 2010***

Omomorfismi di anelli $A \to B$: definizione e proprietá (il nucleo é un ideale di A, l'immagine é un sottoanello di B, l'immagine di un elemento invertibile é un elemento invertibile, mentre l'immagine di uno zero divisore puo' non essere uno zero divisore. La controimmagine di un ideale in un omomorfismo di anelli é un ideale, l'immagine di un ideale in generale non é un ideale, lo é se l'omomorfismo é suriettivo. Esempi. Omomorfismi di gruppi e omomorfismi di anelli da Z_m a Z_n. Ogni omomorfismo di anelli da un campo ad un anello non nullo é iniettivo.
Isomorfismi di anelli. Se due anelli A e B sono isomorfi, allora un elemento é zero-divisore (rispett. é invertibile) in A se e solo se la sua immagine in B é uno zero-divisore (rispett. é invertibile); quindi A é un dominio d'integritá (rispett. é un campo) se e solo se lo é B. L'anello prodotto diretto $R \times R$ e il campo complesso non sono isomorfi. Se due campi A e B sono isomorfi, allora anche i gruppi moltiplicativi (A, .) e (B∗, .) sono isomorfi.*

Ore 2 (9-11) ***Firma (Mirella Manaresi)***

Luogo (Aula) ***Aula Cremona***

Data ***30 novembre 2010***

Svolgimento di un esercizio sugli anelli. Struttura di anello sull'insieme quoziente A/R_f dove $f : A \to B$ é un omomorfismo di anelli commutativi unitari e R_f é la relazione di equivalenza associata a f. Teorema di isomorfismo per anelli commutativi e unitari. Omomorfismo di anelli $Z \to Z_m \times Z_n$ con m, n primi tra loro e isomorfismo indotto $Z_{mn} \to Z_m \times Z_n$. Funzione di Eulero e sua moltiplicativitá; calcolo della funzione di Eulero per ogni intero. Esercizi sugli anelli.

Ore 2 (9-11) ***Firma (Mirella Manaresi)***

Luogo (Aula) ***Aula Cremona***

Data ***1 dicembre 2010***

Omomorfismo da Z ad un anello qualunque A. Sottoanello fondamentale di un anello. Caratteristica di un anello e sottoanello fondamentale. La caratteristica di un dominio d'integritá o é zero o é un primo. Esempi.
Esercizi. L'intersezione di ideali é un ideale, l'unione di ideali non e' un ideale. Ideale somma di due ideali. Gli ideali di un anello prodotto diretto sono tutti e soli i prodotti di ideali.
Polinomi a coefficienti in un anello A: definizioni, somma e prodotto di due polinomi, struttura di anello su $A[x]$. Se A é un dominio allora il grado di un prodotto é la somma dei gradi. L'anello $A[x]$ é un dominio d'inegritá se e solo se A é un dominio d'integritá. Elementi invertibili di $A[x]$ con A dominio. Esempi nel caso in cui A non e' un dominio. Polinomi e funzioni polinomiali.

Ore 2 (9-11) ***Firma (Mirella Manaresi)***

Luogo (Aula) ***Aula Tonelli***

Data ***2 dicembre 2010***

Polinomi a coefficienti in un campo: elementi invertibili, elementi irriducibili. Lemma di divisione. Massimo comun divisore di polinomi. Gli ideali di $K[x]$ con K campo sono tutti principali. Due generatori dello stesso ideale sono tra loro associati. Ogni polinomio non nullo é associato ad un unico polinomio monico. Esistenza del massimo comun divisore di due polinomi non entrambi nulli. Un massimo comun divisore di due polinomi non entrambi nulli f, g é un generatore dell'ideale $(f, g) \subset K[x]$ e si puo' scrivere come combinazione dei due polinomi. Esempi ed esercizi.

Ore 2 (9-11) ***Firma (Mirella Manaresi)***

Luogo (Aula) ***Aula Cremona***

Data ***7 dicembre 2010***

Decomposizione di un polinomio di grado positivo in un prodotto di potenze di polinomi irriducibili distinti.
Radici di un polinomio. Un elemento $a \in K$ é una radice di f se e solo se il polinomio $x - a$ divide f in $K[x]$. Molteplicitá di una radice. Un polinomio irriducibile in $K[x]$ ha una radice se e solo se ha grado 1. Decomposizione in irriducibili e radici di un polinomio. La somma delle molteplicitá delle radici di un polinomio f é minore o uguale al grado di f e vale l'uguaglianza se e solo se il polinomio si spezza in fattori lineari. Questo risultato non vale se K non é un campo.
Campi algebricamente chiusi e loro caratterizzazioni. Enunciato del teorema fondamentale dell'algebra (il campo complesso é un campo algebricamente chiuso). Un campo finito non é mai algebricamente chiuso.
Se il campo K é infinito, due polinomi assumono gli stessi valori in tutti gli elementi di K se e solo se sono uguali. Se il campo K é finito con q elementi, due polinomi assumono gli stessi valori in tutti gli elementi di K se e solo la loro differenza é divisibile per il polinomio $x^q - x$ in $K[x]$.

Ore 2 (9-11) ***Firma (Mirella Manaresi)***

Luogo (Aula) ***Aula Tonelli***

Data ***9 dicembre 2010***

Esercizi su radici dei polinomi e loro molteplicitá, algoritmo della divisione, decomposizione in irriducibili, ideali di $K[x]$.
Radici razionali di un polinomio intero. Legame tra riducibilitá di un polinomio ed esistenza di radici per polinomi di grado maggiore o uguale a due. Radici di un polinomio di grado due su un campo di caratteristica diversa da due. Polinomi reali irriducibili.

Ore 2 (9-11) ***Firma (Mirella Manaresi)***

Luogo (Aula) ***Aula Cremona***

Data ***15 dicembre 2010***

Se un polinomio reale ha una radice complessa α, allora ha anche la radice complessa coniugata $\bar{\alpha}$ e la molteplicitá di α é la stessa di $\bar{\alpha}$. Ogni polinomio reale si decompone in un prodotto di polinomi lineari e di polinomi quadratici con discriminante negativo.
Quadrati e non quadrati in un campo finito. Su ogni campo finito vi sono polinomi di grado due irriducibili. Polinomi irriducibili su Z_2 di grado minore o uguale a cinque.
Esercizi su radici di polinomi a coefficienti in Z_p.

Ore 2 (9-11) ***Firma (Mirella Manaresi)***

Luogo (Aula) ***Aula Tonelli***

Data ***16 dicembre 2010***

Soluzioni di esercizi di vecchie prove d'esame su richiesta degli studenti.

Ore 2 (9-11) ***Firma (Mirella Manaresi)***

Luogo (Aula) ***Aula VII piano***

Data ***20 dicembre 2010***

Soluzioni di esercizi di vecchie prove d'esame su richiesta degli studenti.

Ore 2 (11-13) ***Firma (Mirella Manaresi)***

Luogo (Aula)

Data

Ore ( ) ***Firma***