ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

Anno Accademico *2009/2010*

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) **prof. Monica Idá**

Data inizio Lezioni *6 ottobre 2009*

Data fine Lezioni *21 dicembre 2009*

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 Tonelli***

Data ***6 ottobre 2009***

Introduzione al corso: obiettivi, modalitá d'esame, ricevimento studenti, informazioni varie.
Minimo di un sottoinsieme di Z. Esempi. Principio del minimo. Principio di induzione matematica. Esempi di applicazione del principio di induzione. Esercizi.
Coefficienti binomiali $\binom{n}{k}$.

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

Luogo (Aula) ***AulaTonelli***

Data ***7 ottobre 2009***

Proprietá dei coefficienti binomiali. I coefficienti binomiali sono interi. 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.

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

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

Data ***8 ottobre 2009***

Fattorizzazione di un intero positivo in un prodotto di primi. Massimo comun divisore di due interi. Lemma di divisione. Esistenza del massimo comun divisore e sua espressione come combinazione lineare dei due interi.

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

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

Data ***13 ottobre 2009***

Alcune conseguenze dell'esistenza del massimo comun divisore e della sua espressione come combinazione dei due interi. Teorema Fondamentale dell'Aritmetica.
Alcune note storiche sui numeri primi: crivello di Eratostene, congettura di Gauss, Teorema dei numeri primi, congettura di Golbach, congettura dei primi gemelli.
L'algoritmo euclideo per la determinazione del massimo comun divisore di due interi.

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

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

Data ***14 ottobre 2009***

Brevi richiami su insieme delle parti di un insieme, relazioni, applicazioni tra insiemi, immagine e controimmagine di sottoinsiemi, fibre di una applicazione.
Relazioni di equivalenza. Esempi, in particolare la relazione di equivalenza R_f *su* X *associata ad una applicazione* f *da* X *ad* Y. *Classi di equivalenza. Partizioni su un insieme. La partizione associata ad una relazione di equivalenza.*

Ore 2 (9-11) ***Firma (Monica Idá)***

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

Data ***15 ottobre 2009***

Esercizi sul M.C.D. di due interi. L'equazione diofantea $ax + by = c$ *con* a, b, c *interi.*
Conguenze 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. *Comportamento della relazione di congruenza rispetto a somma, prodotto e potenze. Piccolo teorema di Fermat.*

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

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

Data ***20 ottobre 2009***

Seconda formulazione del piccolo teorema di Fermat; equivalenza delle due formulazioni.
Criteri di divisibilitá per $3, 4, 5, 9, 11$.
Classi di congruenza modulo m, *l'insieme quoziente* Z_m; *operazioni di somma e prodotto fra classi e loro proprietá. Caratterizzazione degli elementi invertibili rispetto al prodotto. Esempi.*

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

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

Data ***21 ottobre 2009***

Richiami su: funzioni suriettive, iniettive, biettive; diagrammi commutativi. La relazione di equivalenza associata ad una partizione su un insieme. Insieme quoziente. Esempi. Se R_f *e' la relazione di equivalenza su* X *associata ad una applicazione* $f : X \to Y$, *gli elementi di* X/R_f *sono le fibre di* f. *La condizione necessaria e sufficiente affinché una funzione passi al quoziente modulo una relazione di equivalenza.*

Ore 2 (9-11) ***Firma (Monica Idá)***

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

Data ***22 ottobre 2009***

La congruenza $ax \equiv b$ (mod 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, congruenze.

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

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

Data ***27 ottobre 2009***

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

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

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

Data ***28 ottobre 2009***

Una applicazione di insiemi f da X ad Y passa sempre al quoziente modulo la relazione di equivalenza R_f su X associata ad f e questo permette sempre di fattorizzare f come composizione di una funzione iniettiva e di una suriettiva.
L'insieme $S(X)$ delle biezioni su un insieme non vuoto X con l'operazione di composizione: vale la proprietá associativa, esiste un elemento, l'identitá, che non ha effetto sulla composizione, ogni biezione ha un'inversa che é ancora una biezione: questo é un esempio di gruppo. Se $X = 1, 2, ..., n$, $S(X)$, denotato con S_n, é detto gruppo simmetrico su n lettere e ha $n!$ elementi. Comporre due permutazioni. Studio del gruppo simmetrico per $n = 3$: descrizione degli elementi, concetto di ciclo, un ciclo di lunghezza 2 ha quadrato uguale all'identitá, un ciclo di lunghezza 3 ha cubo uguale all'identitá; costruzione della tavola di moltiplicazione.

Ore 2 (9-11) ***Firma (Monica Idá)***

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

Data ***29 ottobre 2009***

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.

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

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

Data ***3 novembre 2009***

Calcolo dell'ordine di elementi di gruppi, in particolare calcolo dell'ordine di $[a]_m$ nel gruppo $(Z, +)$ e dell'ordine di elementi di $(Z_m{}^*, .)$. 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. Calcolo dell'ordine di elementi di gruppi prodotto diretto. Sottogruppi: definizione ed esempi. Sottogruppo generato da un elemento. Sottogruppi di $(Z, +)$.

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

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

Data ***4 novembre 2009***

Studio del gruppo simmetrico S_3 utilizzando la sua tavola di moltiplicazione: non commutativitá del gruppo (da cui segue la non commutativitá di S_n per ogni $n > 2$), sottogruppi ciclici di S_3 generati dalle trasposizioni e dai cicli di lunghezza 3, ordine di tali sottogruppi e ordine dei cicli di S_3, sistemi di generatori per S_3. Definizione di ciclo in S_n e prime proprietá.

Ore 2 (9-11) ***Firma (Monica Idá)***

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

Data ***5 novembre 2009***

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. Q e $Z_m \times Z_m$ non sono ciclici. 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.

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

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

Data ***10 novembre 2009***

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 ed esercizi.

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

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

Data ***11 novembre 2009***

Ordine di un ciclo e ordine di un prodotto di cicli disgiunti nel gruppo simmetrico. Orbite di una permutazione: definizione e proprietá. Ogni permutazione diversa dall'identitá é prodotto di cicli disgiunti.

Ore 2 (9-11) ***Firma (Monica Idá)***

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

Data ***12 novembre 2009***

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.

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

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

Data ***17 novembre 2009***

Omomorfismi di gruppi; definizione e prime proprietá. Esempi. Nucleo e immagine di un omomorfismo di gruppi. Isomorfismi. L'applicazione inversa di un isomorfismo e' un omomorfismo di gruppi. La relazione di isomorfismo é una relazione di equivalenza sull'insieme di tutti i gruppi. 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. Un omomorfismo di gruppi da un gruppo ciclico G ad un gruppo H e' determinato dall'immagine di un generatore di G. L'immagine omomorfa di un gruppo ciclico é un gruppo ciclico. Omomorfismi da Z ad un gruppo G. Omomorfismi da Z_m ad un gruppo G.

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

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

Data ***18 novembre 2009***

Ogni permutazione di $S_n, n > 1$, é prodotto di traposizioni. Esempi sulla non unicitá di tale decomposizione. Se una permutazione é prodotto sia di k che di h traposizioni, k e h sono congrui $\bmod 2$. Segno di una permutazione. L'applicazione segno é un omomorfismo di gruppi da S_n al gruppo moltiplicativo $1, -1$, ed il suo nucleo é il gruppo alterno su n lettere A_n. L'ordine di A_n é $n!/2$. Una permutazione é pari se e solo se nella sua decomposizione in cicli disgiunti compare un numero pari di cicli di lunghezza pari.

Ore 2 (9-11) ***Firma (Monica Idá)***

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

Data ***19 novembre 2009***

Esercizi sugli omomorfismi di gruppi (omomorfismi da Z a S_n, da Z_m a S_n, da $Z_m \times Z_m$ a S_n). L'immagine di un sottogruppo é un sottogruppo, la controimmagine di un sottogruppo é un sottogruppo. Se due elementi commutano, allora commutano anche le loro immagini mediante un omomorfismo. Proprietá che si conservano per isomorfismo. Teorema fondamentale di isomorfismo per gruppi. Ogni gruppo ciclico infinito é isomorfo a Z, ogni gruppo ciclico finito é isomorfo a Z_m.

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

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

Data ***24 novembre 2009***

Esercizi sui gruppi.
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. Elementi invertibili di un anello. Campi.

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

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

Data ***25 novembre 2009***

Esercizio sugli omomorfismi di gruppi. Esercizio sugli anelli.
Ideali di un anello. 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. Ideali primi e ideali massimali. Ideali primi e ideali massimali di Z. Esercizi sugli ideali.

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

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

Data ***26 novembre 2009***

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 tuttti e soli i prodotti di ideali; ideali massimali di un anello prodotto diretto. Omomorfismi di anelli. Esempi. Omomorfismi di gruppi e omomorfismi di anelli da Z_m a Z_n. Esercizi su omomorfismi di anelli.

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

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

Data ***1 dicembre 2009***

Svolgimento di un esercizio sugli anelli.
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.
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.*
Teorema di ismorfismo per anelli commutativi e unitari. Omomorfismo da Z ad un anello qualunque A. Sottoanello fondamentale di un anello.

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

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

Data ***2 dicembre 2009***

Caratteristica di un anello e sottoanello fondamentale. La caratteristica di un dominio d'integritá o é zero o é un primo.
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.
Polinomi a coefficienti in un anello A: definizioni, somma e prodotto di due polinomi, struttura di anello su $A[x]$.

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

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

Data ***3 dicembre 2009***

Correzione di un esercizio assegnato.
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.
Elementi irriducibili in un anello. Esempi.
Polinomi a coefficienti in un campo: elementi invertibili, elementi irriducibili. Lemma di divisione. Massimo comun divisore di polinomi.

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

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

Data ***9 dicembre 2009***

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. Decomposizione di un polinomio di grado positivo in un prodotto di potenze di polinomi irriducibili distinti.
Radice 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.

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

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

Data ***10 dicembre 2009***

Esercizi sui polinomi.
Legame tra riducibilitá di un polinomio ed esistenza di radici. 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 $K[x]$.
Derivata di un polinomio.

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

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

Data ***15 dicembre 2009***

Proprietá della derivata di un polinomio su un campo di caratteristica zero. Derivata di un polinomio e radici multiple.
Esercizi sui polinomi, le loro radici, la decomposizione in irriducibili, gli ideali di $K[x]$.

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

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

Data ***16 dicembre 2009***

Correzioni di esercizi di vecchie prove d'esame su anelli prodotto e anelli di polinomi (a richiesta degli studenti).

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

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

Data ***17 dicembre 2009***

Correzioni di esercizi di vecchie prove d'esame (a richiesta degli studenti).

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

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

Data ***21 dicembre 2009***

Correzioni di esercizi di vecchie prove d'esame (a richiesta degli studenti).

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

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

Data

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

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

Data

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

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

Data

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