DIARIO DELLE LEZIONI DI ALGEBRA I

Canale I-Z – A.A. 2013-14

Giovedì 6 Marzo

Introduzione alla teoria degli insiemi: nozioni e notazioni fondamentali. Criterio di uguaglianza tra insiemi. Unione, intersezione e differenza di due o più insiemi. L'insieme vuoto. Leggi di De Morgan. L'insieme delle parti di un insieme dato. L'insieme delle parti dell'insieme vuoto. Prodotto cartesiano di due o più insiemi. Definizione di relazione tra due insiemi. Definizione di funzione (dal punto di vista del suo grafico). Dominio e codominio. Insieme immagine di un sottoinsieme del dominio. Antiimmagine di un sottoinsieme del codominio. Restrizione di una funzione. Esempi di funzione: la funzione costante, la funzione identica, la funzione caratteristica. Definizione di iniettività e suriettività. Biezioni. Insiemi equipotenti. Insiemi finiti.

Lunedì 10 Marzo

Caratterizzazione dell'iniettività e suriettività mediante l'antiimmagine di un elemento del codominio. L'essere equipotenti tra insiemi finiti ed infiniti: osservazioni. Composizione di funzioni: associatività. Composizione di funzioni iniettive (suriettive) è iniettiva (suriettiva). Teorema di caratterizzazione delle funzioni biettive e definizione della funzione inversa. Composizione di funzioni biettive è biettiva e determinazione dell'inversa di $g \circ f$. Relazione riflessiva, simmetrica, transitiva ed anti-simmetrica. Definizione di relazione d'equivalenza. Esempi noti e non noti: il parallelismo tra rette, la similitudine tra matrici, l'equipollenza tra vettori dello spazio, l'orientazione di uno spazio vettoriale reale. Definizione di preordine e di ordine parziale e totale. Insiemi parzialmente e totalmente ordinati. Costruzione di una relazione d'ordine su di un insieme arbitrario. Relazione di divisibilità in $\mathbb{Z}$ ed in $\mathbb{N}$. L'insieme $(\mathcal{P}(X), \subseteq)$ è parzialmente ordinato.

Martedì 11 Marzo

Esercizi su funzioni iniettive e suriettive e sulle relazioni di equivalenza. Definizione di classe di equivalenza di un elemento x rispetto ad una relazione di equivalenza $\sim$. Definizione di classe di equivalenza. Definizione

di partizione. Una relazione di equivalenza su di un insieme genera una partizione. L'insieme quoziente. Rappresentanti di una classe di equivalenza e sistema di rappresentanti.

Giovedì 13 Marzo

Teorema sull'esistenza di una biezione tra l'insieme delle equivalenze e quello delle partizioni di un insieme dato. La congruenza modulo un intero. L'equivalenza definita mediante l'uguaglianza delle immagini ($\sim_f$). La proiezione di un insieme sul quoziente. Enunciato e dimostrazione del Teorema principale che lega equivalenze e funzioni e suo corollario. Introduzione alla definizione di cardinalità: contare sul finito e sul non finito. Definizione di insieme numerabile. Equipotenza tra $\mathbb{N}$ e $\mathbb{Z}$. Confronto tra insiemi: definizione di $\leq$ sull'insieme Card delle cardinalità. La definizione è ben posta. Teorema di Schroeder-Bernstein (senza dimostrazione). $(\mathrm{Card}, \leq)$ è un insieme totalmente ordinato.

Lunedì 17 Marzo

$|X| \leq |Y|$ se, e solo se, esiste $f : Y \longrightarrow X$ suriettiva: definizione equivalente. Un insieme infinito contiene sempre un sottoinsieme numerabile. Assioma della scelta e Lemma di Zorn (semplice accenno). Un sottoinsieme di un insieme numerabile è finito o numerabile. $|\mathbb{N}|$ è la più piccola delle cardinalità non finite. L'unione di un numero finito o di un'infinità numerabile di insiemi numerabili è numerabile: la diagonale di Cantor. L'unione di un numero finito o di un'infinità numerabile di insiemi finiti o numerabili è finita o numerabile. La cardinalità di $\mathbb{Z}$, $\mathbb{Q}$ e $A \times B$. Teoremi di Cantor: $|A| < |\mathcal{P}(A)|$, $|\mathbb{R}| = |(0,1)| = |[0,1)| = |\{0,1\}^{\mathbb{N}}| = |\mathcal{P}(\mathbb{N})|$, quindi $|\mathbb{N}| < |\mathbb{R}|$. L'ipotesi del continuo e l'ipotesi del continuo generalizzata. Un insieme infinito ammette una partizione in sottoinsiemi tutti numerabili (senza dimostrazione). Se X è un insieme infinito $|X \times \mathbb{N}| = |X| = |X \times X|$ (l'ultima uguaglianza senza dimostrazione). Osservazione sul preordine e l'ordine su di un insieme.

Martedì 18 Marzo

Esercizi sulle equivalenze e sulle cardinalità. I numeri algebrici. La cardinalità di un'unione numerabile di insiemi X_n tali che $|X_n| \leq |X_0|$ per ogni

n. Alcune osservazioni e precisazioni sulla definizione di cardinalità. Introduzione alle strutture algebriche. Costruzione su insiemi finiti qualsiasi per mezzo delle tavole di Cayley. I numeri interi: Assiomi di Peano. Principio di induzione. Principio del buon ordinamento.

Giovedì 20 Marzo

Principio di induzione forte. Equivalenze tra principio d'induzione, induzione forte e buon ordinamento. Cenni sulla costruzione di $\mathbb{Z}$. Definizione di opeazione su di un insieme e di struttura algebrica. Semigruppo, monoide, gruppo e gruppo abeliano. Esempi. Unicità dell'elemento neutro e dell'inverso. Il gruppo simmetrico su di un insieme. Definizione di sottostruttura e sottogruppo. Il sottogruppo degli elementi invertibili di un monoide. Definizione di anello, dominio, corpo e campo. Struttura moltiplicativa dell'anello. Divisori dello zero. Un dominio è privo di divisori dello zero. Cancellazione in un dominio.

Lunedì 24 Marzo

Ancora sui domini. Esempi. Un dominio d'integrità finito è un campo. Divisione col resto in $\mathbb{Z}$: proprietà euclidea degli interi. Esistenza ed unicità del mcd tra interi. Identità di Bezout. Condizioni necessarie e sufficienti affinchè due interi siano coprimi. Teorema dell'algoritmo euclideo ed applicazione.

Martedì 25 Marzo

Esercizi sul principio d'induzione e sul mcd. Definizione di numero primo. Proprietà semplici del mcd e dei primi. Lemma di Euclide e sua generalizzazione. Preparazione al Teorema fondamentale dell'aritmetica. Dimostrazione del Teorema. $\mathbb{P}$ è infinito.

Giovedì 27 Marzo

Introduzione all'aritmetica congruenziale. Compatibilità della congruenza modulo m con le operazioni di somma e moltiplicazione. Divisione col resto per numeri grandi. Operazioni in $\mathbb{Z}/\equiv_m$. $\mathbb{Z}/\equiv_m$ è un anello commutativo unitario. Gli elementi invertibili di $\mathbb{Z}/\equiv_m$: caratterizzazione.

Condizioni necessarie e sufficienti affinchè $\mathbb{Z}/\equiv_m$ sia un campo. La funzione di Eulero. Gruppi ciclici. Esempi: $(\mathbb{Z}/\equiv_m, \hat{+})$ e $(\mathbb{Z}, +)$. I generatori di $(\mathbb{Z}/\equiv_m, \hat{+})$. Teorema di Eulero-Fermat: dimostrazione utilizzando il risultato sui gruppi abeliani. Piccolo Teorema di Fermat. Applicazioni (in negativo) e numeri pseudoprimi. Teorema di Wilson.

Lunedì 31 Marzo

Equazioni congruenziali. Condizioni necessarie e sufficienti e soluzioni di un'equazione congruenziale. Sistemi di equazioni congruenziali. Teorema Cinese del Resto. Esercizi sulle congruenze ed i sistemi di equazioni congruenziali.

Martedì 1 Aprile

Ancora esercizi sulle congruenze. Criteri di divisibilità. Introduzione alla teoria degli gruppi. Richiami della definizione ed esempi. Definizioni di omo-/epi-/monomorfismo tra strutture. Strutture isomorfe. Endomorfismi ed automorfismi. L'automorfo di una struttura algebrica. Proprietà semplici degli isomorfismi tra strutture. L'immagine dell'elemento neutro di un gruppo tramite un omomorfismo di gruppi e dell'unità (moltiplicativa) di un anello tramite un omomorfismo di anelli. Sottogruppi di un gruppo: caratterizzazione. Intersezioni di sottogruppi. Struttura generata da un insieme di elementi di una struttura data. Sottogruppo generato. I sottogruppi banali G e $\{1_G\}$

Giovedì 3 Aprile

I sottogruppi di $(\mathbb{Z}, +)$. La relazione $\sim_H$. Il Teorema di Lagrange sull'ordine dei sottogruppi di un gruppo finito. Indice di un sottogruppo nel gruppo. Classi laterali destre e sinistre. Congruenze. Sottogruppi normali e congruenze. Sottogruppi banali e sottogruppi normali di un gruppo abeliano. I sottogruppi di indice 2 sono normali. Il gruppo quoziente (rispetto ad un sottogruppo normale). L'immagine di un gruppo tramite un omomorfismo è un sottogruppo. Il nucleo di un omomorfismo. f è iniettiva se, e solo se, $\mathrm{Ker} f = \{1_G\}$. L'epimorfismo canonico. Teorema di fattorizzazione. Teorema di omomorfismo per gruppi.

Lunedì 7 Aprile

Teorema di corrispondenza per i sottogruppi del gruppo quoziente. Anti-immagine ed immagine di un sottogruppo normale tramite un omomorfismo. Applicazione del teorema di omomorfismo. Il gruppo simmetrico: scrittura standard e rappresentazione figurata di una permutazione. Insieme dei punti fissi, π-orbita, cicli, trasposizioni, cicli disgiunti. Esempi. Commutatività di due cicli disgiunti.

Martedì 8 Aprile (Lezione di recupero)

Esercizi sui gruppi: applicazione del Teorema di omomorfismo, quando l'unione e/o il prodotto di sue sottogruppi è un sottogruppo. Il centro di un gruppo ed il gruppo degli automorfismi interni. $G/Z(G)$ è isomorfo a $\mathrm{Inn}(G)$.

Giovedì 10 Aprile

Commutatività di un numero arbitrario di cicli disgiunti. Cardinalità di una π-orbita. La relazione di coniugio in un gruppo. Centralizzante di un elemento. Permutazioni coniugate. Ogni permutazione ammette un'unica decomposizione in cicli disgiunti. Ogni permutazione è prodotto di trasposizioni. La struttura ciclica di una permutazione. Due permutazioni hanno la stessa struttura ciclica se, e solo se, sono coniugate.

Lunedì 14 Aprile

Costruzione del gruppo alterno. Segnatura di una permutazione. Permutazioni pari e dispari. Il Teorema di Cayley. Ordine degli elementi di un gruppo. L'ordine di un elemento divide l'ordine del gruppo. Generatori di gruppi e sottogruppi: caso abeliano e non abeliano. Per ogni gruppo ciclico G esiste $n \in \mathbb{N}$ tale che G è isomorfo a $(\mathbb{Z}/\equiv_n, \hat{+})$. Ogni quoziente ed ogni sottogruppo di un gruppo ciclico è ciclico. Se G è un gruppo ciclico di ordine n, per ogni d divisore di n esiste esattamente un sottogruppo ciclico di ordine d. Se G ha ordine p^r i sottogruppi formano una catena. Proprietà sommatoria della funzione di Eulero.

Martedì 15 Aprile

Ancora esercizi sui gruppi. L'immagine del centro di un gruppo tramite un automorfismo. Il Teorema del parallelogramma. Caratterizzazione dei gruppi ciclici finiti.

Lunedì 5 Maggio

Richiami sugli anelli ed esempi di omomorfismi. Sottoanelli ed ideali di un anello. Caratterizzazione dei sottoanelli di un anello. Gli ideali di $\mathbb{Z}$. L'immagine di un anello tramite un omomorfismo è un sottoanello. Il nucleo di un omomorfismo. f è iniettiva se, e solo se, $\mathrm{Ker} f = \{0\}$. Sottostrutture generate. Ideale generato. Generatori di ideali. Ideali principali. Anelli di tipo finito. Domini ad ideali principali. Gli ideali di un corpo. Descrizione dell'ideale generato da un numero finito di elementi in un anello commutativo unitario. Costruzione dell'anello quoziente (rispetto ad un ideale). L'epimorfismo canonico. Teorema di fattorizzazione. Teorema di omomorfismo per anelli. Antiimmagine di un ideale ed immagine di un ideale tramite un epimorfismo.

Martedì 6 Maggio

Teorema di corrispondenza per gli anelli fattoriali. Ideali primi ed ideali massimali: caratterizzazione in un anello commutativo unitario. Massimale implica primo. Caratteristica di un anello. la caratteristica di un campo è 0 o un numero primo p. Esercizi su sottoanelli unitari e non di un anello unitario ed applicazione del Teorema di omomorfismo.

Giovedì 8 Maggio

Il campo dei quozienti o delle frazioni di un dominio: costruzione del campo dei quozienti. Il problema dell'immersione di un dominio in un campo: la proprietà universale del campo dei quozienti e precisazione sull'unicità. L'anello dei polinomi: non si può sempre pensare un polinomio come ad una funzione in una variabile. Un polinomio come successione definitivamente nulla. Costruzione dell'anello dei polinomi. Ampliamento di un anello: l'anello $A[z]$. Elemento algebrico e trascendente: differenze. L'estensione dell'anello $\{(a, 0, \ldots, 0, \ldots) | \, a \in A\}$ per mezzo dell'elemento

$x := (0, 1, 0, \ldots, 0, \ldots)$ è l'anello dei polinomi $A[x]$. Principio di uguaglianza tra polinomi.

Lunedì 12 Maggio

Immersione di un anello in un anello dei polinomi: la proprietà universale dell'anello dei polinomi. Grado di un polinomio non nullo, coefficiente lineare, direttore e termine noto. Divisibilità tra polinomi. Polinomi irriducibili. Grado della somma e del prodotto tra polinomi. Se A è un dominio, allora $A[x]$ è dominio e $\mathcal{U}(A[x]) = \mathcal{U}(A)$. Anello dei polinomi in più variabili: definizione induttiva. La proprietà euclidea dei polinomi monici e sua estensione al caso di anello dei polinomi a coefficienti in un campo. Definizione di funzione euclidea e di dominio euclideo (DE). Esempi: $(\mathbb{Z}, |\ |)$, $(C[x], \delta)$, gli interi di Gauss $\mathbb{Z}[i]$, un qualsiasi campo C.

Martedì 13 Maggio

Esercizi su ideali primi e massimali ed applicazioni del Teorema di omomorfismo per anelli. Gli elementi invertibili di $\mathbb{Z}[i]$. C campo se, e solo se, δ è funzione euclidea su $C[x]$. Definizione di dominio ad ideali principali (DIP). $\mathbb{Z}[x]$ non è DIP. DE implica DIP.

Giovedì 15 Maggio

Dimostrazione del fatto che DE implica DIP. Quindi $C[x]$ è DIP. I generatori di un ideale J di $C[x]$ e descrizione dell'anello quoziente $C[x]/J$. J è massimale se, e solo se, J è primo se, e solo se, J è generato da un polinomio irriducibile. Introduzione ai criteri di irriducibilità per i polinomi. Se C è un campo ogni polinomio di grado 1 è irriducibile. Polinomi irriducibili in $\mathbb{C}[x]$ e $\mathbb{R}[x]$. $\mathbb{Q}[x]$ ammette polinomi irriducibili di grado qualsiasi. Polinomi irriducibili in $\mathbb{Q}[x]$, ma non in $\mathbb{Z}[x]$. Irriducibilità in $\mathbb{Z}[x]$ implica irriducibilità in $\mathbb{Q}[x]$ se il grado è diverso da zero. Criterio di Eisenstein. Criterio di traslazione. Criterio di irriducibilità di un polinomio di grado 2 o 3 a coefficienti in un campo. Possibili radici in $\mathbb{Q}$ di un polinomio a coefficienti in $\mathbb{Z}$. Teorema di riduzione modulo un primo. Divisibilità in un dominio. Elementi primi, irriducibili ed associati.

Lunedì 19 Maggio

Formulazioni equivalenti dei concetti di elementi primi, irriducibili ed associati e loro interpretazioni in termini di ideali generati. a primo implica a irriducibile ed equivalenza in un dominio a ideali principali. In un DIP ogni ideale primo non banale è massimale. Definizione di dominio atomico e di dominio a fattorizzazione unica (DFU). Esempi. Domini a fattorizzazione unica: fissare gli irriducibili. A è DFU se, e solo se, A è atomico e ogni $p \in A$ irriducibile è primo. Condizione delle catene ascendenti per gli ideali (principali) di un anello. Anello a condizione massimale per i suoi ideali (principali). A verifica la condizione delle catene ascendenti se, e solo se, è a condizione massimale per i sui ideali se, e solo se, è di tipo finito.

Martedì 20 Maggio

Esercizi sugli anelli, su ideali primi e massimali. MCD tra elementi di un dominio. L'MCD è una classe di equivalenza rispetto alla relazione di associato. Esistenza dell'MCD nei DFU. L'MCD nei DIP e ideali generati. Identità di Bezout generalizzata. Elementi coprimi. Teorema dell'algoritmo euclideo per trovare un elemento dell'MCD nei DE. Esercizi.

Giovedì 22 Maggio

Se A è DIP, allora A è a condizione massimale per i suoi ideali e ogni irriducibile è primo. A è DFU se, e solo se, A è a condizione massimale per i suoi ideali principali e ogni $p \in A$ irriducibile è primo. DIP implica DFU. Fattorizzazione in $C[x]$, dove C è un campo: il problema delle radici di un polinomio. Teorema di Ruffini. Teorema di Cauchy. Teorema fondamentale dell'Algebra (senza dimostrazione). Contenuto di un polinomio a coefficienti interi e polinomi primitivi. Decomposizione (unica) di un polinomio a coefficienti razionali nel prodotto di un numero razionale positivo e di un polinomio primitivo. Lemma di Gauss. Divisibilità tra polinomi in $\mathbb{Z}[x]$ ed in $\mathbb{Q}[x]$: relazioni.

Lunedì 26 Maggio

Dimostrazione dell'irriducibilità in $\mathbb{Q}[x]$ di un polinomio (a coefficienti interi) di grado ≥ 1 irriducibile in $\mathbb{Z}[x]$. Dimostrazione del Criterio di Eisenstein. Gli elementi irriducibili di $\mathbb{Z}[x]$. f irriducibile in $\mathbb{Z}[x]$ implica f

elemento primo di $\mathbb{Z}[x]$. $\mathbb{Z}[x]$ è DFU. $\mathbb{Z}[\sqrt{10}]$ non è DFU: esistono elementi irriducibili, ma non primi.

Martedì 27 Maggio

Esercizi sui polinomi: irriducibilità, anello quoziente, Teorema cinese del resto.

Giovedì 29 Maggio

Introduzione dei primi di Gauss. Un numero primo p o è primo di Gauss o è il prodotto di due primi di Gauss complessi e coniugati. Se π è un primo di Gauss, allora o $\pi\overline{\pi}$ è un numero primo, o è il quadrato di un numero primo. Se $p \in \mathbb{P}$, p è un prodotto di due primi di Gauss complessi e coniugati se, e solo se, $p = a^2 + b^2$ (se, e solo se, $x^2 \equiv_p -1$ ha soluzioni) se, e solo se, p è pari o $p \equiv_4 1$. I numeri primi che sono di Gauss sono quindi tutti e soli quelli congrui a 3 (mod 4). Caratterizzazione dei primi di Gauss. Qualche esercizio.

Martedì 3 Giugno

Ancora esercizi sulla fattorizzazione in $\mathbb{Z}[i]$.

Giovedì 5 Giugno (a cura del Dott. Cerulli Irelli)

Ancora esercizi sui domini.

Lunedì 9 Giugno

Seconda prova d'Esonero.

Giovedì 12 Giugno

Visione dei compiti.