**DIARIO DELLE LEZIONI DI ALGEBRA I**

Canale M-Z – A.A. 2015-16

## Martedì 1 Marzo

Presentazione del Corso. 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 ed iterazioni. 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. Composizione di funzioni: associatività. Composizione di funzioni iniettive (suriettive) è iniettiva (suriettiva).

## Giovedì 3 Marzo

Caratterizzazione dell'iniettività e suriettività mediante l'antiimmagine di un elemento del codominio. 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 (matrici associate ad uno stesso endomorfismo o ad uno stesso omomorfismo di spazi vettoriali), l'equipollenza tra vettori dello spazio (differenza tra vettore libero e vettore applicato), l'orientazione di uno spazio vettoriale reale. Definizione di preordine e di ordine parziale e totale. Insiemi parzialmente e totalmente ordinati. Relazione di divisibilità in $\mathbb{Z}$ ed in $\mathbb{N}$. L'insieme $(\mathcal{P}(X), \subseteq)$ è parzialmente ordinato. Definizione di classe di equivalenza di un elemento $x$ rispetto ad una relazione di equivalenza $\sim$. Definizione di classe di equivalenza. Proprietà delle classi di equivalenza.

## Lunedì 7 Marzo

Esercizi su funzioni iniettive e suriettive. 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. 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 del Teorema principale che lega equivalenze e funzioni e suo corollario.

## Martedì 8 Marzo

Dimostrazione del Teorema principale. Esercizi sulle equivalenze. Introduzione al concetto di cardinalità: contare sul finito e sul non finito. Insiemi aventi la stessa cardinalità ed osservazioni. Equipotenza tra $\mathbb{N}$ e $\mathbb{Z}$: un sottinsieme infinito contiene un sottoinsieme proprio della stessa cardinalità. Confronto tra insiemi: quando $|X| \leq |Y|$. Osservazioni.

## Giovedì 10 Marzo

Teorema di Schroeder-Bernstein (senza dimostrazione). Definizione di insieme numerabile. Un insieme infinito contiene sempre un sottoinsieme numerabile. Assioma della scelta e Lemma di Zorn: definizione di catena, maggioranti ed elemento massimale. Applicazione del Lemma di Zorn: ogni spazio vettoriale ha una base. Teorema del buon ordinamento: equivalenza col Lemma di Zorn (senza dimostrazione). Un insieme ben ordinato è totalmente ordinato. Osservazioni sul buon ordinamento. Un sottoinsieme di un insieme numerabile è finito o numerabile. Ogni insieme infinito $X$ è tale che $|\mathbb{N}| \leq |X|$. 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 $|\mathbb{N}| < |\mathbb{R}|$: dimostrazione della prima parte. L'ipotesi del continuo e l'ipotesi del continuo generalizzata.

## Lunedì 14 Marzo

Fine della dimostrazione del Teorema di Cantor. Esercizi sulle cardinalità. I numeri reali algebrici su $\mathbb{Z}$. 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). La cardinalità di un'unione numerabile di insiemi $X_n$ tali che $|X_n| \leq |X_0|$ per ogni $n$ e $X_0$ è infinito. Alcune osservazioni e precisazioni sulla definizione (non data) di cardinalità. I numeri naturali: Assiomi di Peano. Principio di induzione. Costruzione di $\mathbb{Z}$.

## Martedì 15 Marzo

Principio di induzione forte e principio del buon ordinamento. Equivalenze tra principio d'induzione, induzione forte e buon ordinamento. Introduzione alle strutture algebriche: le tavole di Cayley. 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. Esempi. Struttura moltiplicativa dell'anello. Divisori dello zero. Un dominio è privo di divisori dello zero. Cancellazione in un dominio.

## Giovedì 17 Marzo

Ancora sugli anelli. 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. Definizione di numero primo. Proprietà semplici del mcd e dei primi. Lemma di Euclide.

## Lunedì 21 Marzo

Generalizzazione del Lemma di Euclide. Teorema fondamentale dell'aritmetica. $\mathbb{P}$ è infinito. I primi di Mersenne. Esercizi sul principio d'induzione, sulla divisibiltà e sul mcd. Introduzione all'aritmetica congruenziale. Compatibilità della congruenza modulo $m$ con le operazioni di somma e moltiplicazione. Divisione col resto per numeri grandi.

## Martedì 22 Marzo

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: notazione additiva e moltiplicativa. Le potenze di un elemento di un gruppo. 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. Esercizi sulle congruenze.

## Giovedì 31 Marzo

Teorema di Wilson. Ancora esercizi di aritmetica modulare. Equazioni congruenziali. Condizioni necessarie e sufficienti per la risolubilità e soluzioni di un'equazione congruenziale. Sistemi di equazioni congruenziali. Teorema Cinese del Resto. Primi esercizi.

## Lunedì 4 Aprile

Ancora esercizi sui sistemi di equazioni alle congruenze. Equazioni diofantee. 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.

## Martedì 5 Aprile

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. I sottogruppi banali $G$ e $\{1_G\}$. I sottogruppi di $(\mathbb{Z}, +)$. Struttura generata da un insieme di elementi di una struttura data. Sottogruppo generato. Gruppi finitamente generati ed insiemi di generatori. 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. Coniugato di un elemento $x$ mediante un elemento $y$. Sottogruppi

banali e sottogruppi normali di un gruppo abeliano. I sottogruppi di indice 2 sono normali.

## Mercoledì 6 Aprile (in sostituzione di Probabilità I)

Teorema di caratterizzazione dei sottogruppi 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, $\mathrm{Ker} f = \{1_G\}$. La proiezione al quoziente (o epimorfismo canonico). Teorema di fattorizzazione. Teorema di omomorfismo per gruppi. Antiimmagine ed immagine di un sottogruppo normale tramite un omomorfismo. Teorema di corrispondenza per i sottogruppi del gruppo quoziente. I sottogruppi di $\mathbb{Z}/\mathbb{Z}m$.

## Lunedì 11 Aprile

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

## Martedì 12 Aprile

Il Teorema del parallelogramma. Il gruppo simmetrico: scrittura standard e rappresentazione figurata di una permutazione. Insieme dei punti fissi, $\pi$-orbita, cicli, trasposizioni, cicli disgiunti. Esempi. Commutatività di due cicli disgiunti e di un numero arbitrario di cicli disgiunti. Il prodotto di cicli disgiunti. Cardinalità di una $\pi$-orbita.

## Giovedì 14 Aprile

Un ciclo come prodotto di trasposizioni. Il comiugato di un ciclo. Ogni permutazione ammette un'unica decomposizione in cicli disgiunti. Ogni permutazione è prodotto di trasposizioni. La struttura ciclica di una permutazione. Permutazioni simili. Due permutazioni hanno la stessa struttura ciclica se, e solo se, sono simili (e quindi sono coniugate). Il Teorema di Cayley.

## Martedì 26 Aprile

$S_n$ contiene un sottogruppo di indice 2: costruzione del gruppo alterno. Segnatura di una permutazione. Permutazioni pari e dispari. Ordine degli elementi di un gruppo. L'ordine di un elemento divide l'ordine del gruppo. 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.

## Giovedì 28 Aprile

Teorema di caratterizzazione dei gruppi ciclici finiti. Il gruppo alterno $A_4$ ed il reticolo dei suoi sottogruppi: non si inverte il Teorema di Lagrange e l'essere un sottogruppo normale non è una proprietà transitiva. Esercizi sui gruppi. L'automorfo di un gruppo ciclico finito e del gruppo simmetrico $S_3$. Esponente di un gruppo abeliano finito ed esistenza di un elemento di ordine $\exp(G)$.

## Lunedì 2 Maggio

Richiami sugli anelli. Sottoanelli ed ideali di un anello. Caratterizzazione dei sottoanelli di un anello. Gli ideali di $\mathbb{Z}$. 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. L'immagine di un anello tramite un omomorfismo è un sottoanello. Il nucleo di un omomorfismo. $f$ è iniettiva se, e solo se, $\mathrm{Ker} f = \{0\}$. Costruzione dell'anello quoziente (rispetto ad un ideale). La proiezione al quoziente. Teorema di fattorizzazione. Teorema di omomorfismo per anelli. Antiimmagine di un ideale ed immagine di un ideale tramite un epimorfismo.

## Martedì 3 Maggio

Teorema di corrispondenza per i sottoanelli di un quoziente. Esercizi su sottoanelli unitari e non di un anello unitario ed applicazione del Teorema di omomorfismo. Caratteristica di un campo (è 0 o un numero primo $p$).

Ideali primi ed ideali massimali: caratterizzazione in un anello commutativo unitario (senza dimostrazione). Massimale implica primo.

## Giovedì 5 Maggio

Dimostrazione del teorema di caratterizzazione di ideali primi e massimali. Gli ideali massimali di $\mathbb{Z}$. Il campo dei quozienti o delle frazioni di un dominio: costruzione. 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. Grado di un polinomio non nullo, coefficiente lineare, direttore e termine noto. Divisibilità tra polinomi. Polinomi irriducibili.

## Lunedì 9 Maggio

Immersione di un anello in un anello dei polinomi: la proprietà universale dell'anello dei polinomi. 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 $\mathbb{Z}[i]$ con la norma, un qualsiasi campo $C$. $C$ campo se, e solo se, $\delta$ è funzione euclidea su $C[x]$. Definizione di dominio ad ideali principali (DIP). $\mathbb{Z}[x]$ non è DIP. DE implica DIP. Quindi $C[x]$ è DIP. I generatori di un ideale $J$ di $C[x]$ e descrizione dell'anello quoziente $C[x]/J$.

## Martedì 10 Maggio

Esercizi su ideali primi e massimali. Gli ideali massimali di $C[x]$: $J$ è massimale se, e solo se, $J$ è primo se, e solo se, $J$ è generato da un polinomio irriducibile.

## Giovedì 12 Maggio

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. Se un polinomio $f = a_0 + a_1x + \ldots + a_nx^n \in \mathbb{Z}[x]$ è tale che $\mathrm{mcd}(a_0, \ldots, a_n) = 1$ allora è irriducibile in $\mathbb{Q}[x]$ se, e solo se, lo è in $\mathbb{Z}[x]$. Criterio di Eisenstein (senza dimostrazione). Criterio di traslazione (senza dimostrazione). Criterio di irriducibilità di un polinomio di grado 2 o 3 a coefficienti in un campo (senza dimostrazione). Possibili radici in $\mathbb{Q}$ di un polinomio a coefficienti in $\mathbb{Z}$. Teorema di riduzione modulo un primo (senza dimostrazione). Divisibilità in un dominio. Elementi primi, irriducibili ed associati. 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.

## Lunedì 16 Maggio

$A$ 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. 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). Il Teorema di Cauchy non vale se $C$ non è un campo.

## Martedì 17 Maggio

Esercizi su irriducibilità, anelli dei polinomi, quozienti e divisione col resto tra polinomi. Il Teorema cinese dei resti generalizzato. Le radici complesse e coniugate di un polinomio a coefficienti in $\mathbb{R}$: discussione sul

criterio di irriducibilità di un polinmio a coefficienti in $\mathbb{C}[x]$ e $\mathbb{R}[x]$.

## Giovedì 19 Maggio

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.

## Lunedì 23 Maggio

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

## Martedì 24 Maggio

$f$ irriducibile in $\mathbb{Z}[x]$ implica $f$ elemento primo di $\mathbb{Z}[x]$. $\mathbb{Z}[x]$ è DFU. Le definizioni di DE, DIP, DFU non sono mutualmente equivalenti. $\mathbb{Z}[\sqrt{10}]$ non è DFU: esistono elementi irriducibili, ma non primi. Dimostrazione del criterio di irriducibilità di un polinomio modulo un primo.

## Giovedì 26 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 $\pi$ 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.

## Lunedì 30 Maggio

Ancora esercizi sulla fattorizzazione in $\mathbb{Z}[i]$. Il corpo dei quaternioni.

## Martedì 31 Maggio

Prodotto diretto esterno di due gruppi. Proiezioni. Prodotto diretto interno di sottogruppi (normali) di un gruppo. Isomorfismo tra prodotto diretto interno ed esterno. Condizioni necessarie e sufficienti affichè $G$ sia prodotto diretto di suoi sottogruppi. Il gruppo ciclico di ordine $pq$ con $\mathrm{mcd}(p, q) = 1$. Prodotto semidiretto di gruppi. Prodotto diretto come caso particolare del prodotto semidiretto. Prodotto semidiretto ed automorfismi interni. Quando un gruppo è prodotto semidiretto di suoi sottogruppi. Il gruppo simmetrico come prodotto semidiretto. I gruppi diedrali.

## Lunedì 6 Giugno

Domande e saluti.