Elementi di algebra da un punto di vista superiore, AA 2015-2016; Programma svolto.

Semianello ordinato $\mathbb{N}$ dei numeri naturali. Sistemi di Peano; definizioni ricorsive e dimostrazioni per induzione. Due sistemi di Peano sono isomorfi, a meno di un unico isomorfismo. Operazioni di addizione e moltiplicazione, ordine naturale e ordine parziale di divisibilita'; semianello commutativo ordinato $(\mathbb{N}; +, 0; \cdot, 1; \leq)$. Principio del minimo. Divisione euclidea. Numeri primi; lemma di Euclide (en.); teorema fondamentale dell'aritmetica.

Insiemi finiti, cardinalita', combinatoria elementare. Equipotenza, segmenti iniziali di $\mathbb{N}$, insiemi finiti, cardinalita'. Proprieta' della cardinalita' rispetto a inclusione, quozienti, unione disgiunta, unione-e-intersezione, prodotto cartesiano. Conteggio di funzioni, sottinsiemi, funzioni iniettive, permutazioni; fattoriali. Principio del pastore. Coefficienti binomiali come enumeratori di sottinsiemi; altre interpretazioni. Formula ricorsiva, formula esplicita. Teorema binomiale.

Anello ordinato $\mathbb{Z}$ dei numeri interi relativi; anelli commutativi; anelli $\mathbb{Z}_n$ di classi di resti. Una presentazione scolastica dell'anello degli interi relativi. Costruzione formale del gruppo abeliano $(\mathbb{Z}; +, 0, -)$ a partire dal monoide commutativo regolare $(\mathbb{N}; +, 0)$ e dell'anello $(\mathbb{Z}; +, 0, -; \cdot, 1)$ a partire dal semianello $(\mathbb{N}; +, 0; \cdot, 1)$. Ordine naturale. Valore assoluto. Divisione con resto. Teorema fondamentale dell'aritmetica.

Esistenza e unicita' di omomorfismi di monoidi con dominio $\mathbb{N}$ aventi data immagine di 1. Monoide libero su un insieme, esistenza e unicita'. $\mathbb{N}$ come monoide libero sul suo elemento 1. Esistenza e unicita' di omomorfismi di gruppi con dominio $\mathbb{Z}$ aventi data immagine di 1. Gruppo libero su un insieme, esistenza e unicita'. $\mathbb{Z}$ come gruppo libero sul suo elemento 1. Esistenza e unicita' di un omomorfismo di anello da $\mathbb{Z}$ ad ogni altro anello; sottoanello fondamentale di un anello.

Relazione d'equivalenza, partizione, insieme quoziente, proiezione su insieme quoziente. Per gruppi abeliani: sottogruppo, congruenza, gruppo quoziente, proiezione sul gruppo quoziente. Sottogruppo nucleo di una congruenza e congruenza associata a un sottogruppo, classi di congruenza come laterali del nucleo. Caratterizzazione dei sottogruppi, congruenze, e gruppi quoziente di $\mathbb{Z}$, come $n\mathbb{Z}$, congruenze modulo n, gruppi di classi di resti $\mathbb{Z}_n$. Per anelli commutativi: sottoanello, ideale, congruenza, anello quoziente, omomorfismo proiezione sull'anello quoziente. Ideale nucleo di una congruenza e congruenza associata a un ideale, classi di congruenza come laterali del nucleo. Caratterizzazione degli ideali, congruenze, e anelli quoziente di $\mathbb{Z}$, come $n\mathbb{Z}$, congruenze modulo n, anelli di classi di resti $\mathbb{Z}_n$. Regola del 9. Fattorizzazione epi-mono di una funzione fra insiemi. Per anelli commutativi, primo teorema fondamentale di omomorfismo. Caratteristica di un anello, sottoanello fondamentale, e anelli $\mathbb{Z}$ e $\mathbb{Z}_n$. Domini d'integrita' finiti sono campi. Un anello $\mathbb{Z}_n$ e' campo sse n e' primo. Caratteristica di un dominio d'integrita', sottoanello fondamentale, e campi $\mathbb{Z}_p$.

Campo ordinato $\mathbb{Q}$ dei numeri razionali. Campo dei quozienti di un dominio d'integrita', costruzione e proprieta' universale. Campo $\mathbb{Q}$ come campo dei quozienti del dominio $\mathbb{Z}$. Connessioni con presentazioni scolastiche di $\mathbb{Q}$. Struttura di campo e risolubilta' equazioni di I grado. $\mathbb{Q}$ e' campo di caratteristica zero, ordinato, denso, archimedeo,

non completo.

Un anello commutativo e' un campo sse non posiede ideali propri. Ciascun omomorfismo di campi e' iniettivo. Esistenza e unicita' di un monomorfismo da $\mathbb{Q}$ verso ogni altro campo di caratteristica 0.

Anelli di polinomi in una indeterminata. Tutti gli anelli considerati sono tacitamente supposti commutativi. In un anello, sottoanello generato da un sottoanello e un elemento. Per un anello A, definizione dell'anello $A[x]$ dei polinomi a coefficienti in A nell'indeterminata x mediante proprieta' universale rispetto agli anelli con un dato sottoanello copia isomorfa di A ed un dato elemento; omomorfismo di sostituzione. Anello $A[[x]]$ delle serie formali a coefficienti in A nell'indeterminata x. Caratterizzazione degli elementi invertibili. Funzioni generatrici; la funzione generatrice dei numeri di Fibonacci; la funzione generatrice dei coefficienti multinsiemistici. Costruzione di $A[x]$ come sottoanello di $A[[x]]$ delle serie formali con un numero finito di coefficienti non nulli. Polinomi e funzioni polinomiali.

Per A anello, $A[x]$ e' una $A-$algebra, caratterizzata da una proprieta' universale rispetto alle $A-$algebre con un elemento fissato. Per A dominio d'integrita', $A[x]$ e' un dominio d'integrita'. Grado, relazione con operazioni, caratterizzazione dell'invertibilita'. Preordine di divisibilita', relazione d'equivalenza associata. Polinomi irriducibili. Per K campo, $K[x]$ e' una $K-$algebra di dimensione infinita. Invertibilita'; polinomi irriducibili. Divisione con resto. Lemma di Euclide. Teorema di fattorizzazione unica. Irriducibilita' in $\mathbb{Q}[x]$, $\mathbb{Z}[x]$, $\mathbb{Z}_p[x]$. Polinomi primitivi. Lemma di Gauss. Criterio di Eisenstein.

Per K campo, $K[x]$ e' un anello a ideali principali. Per $f(x)$ polinomio di grado $n > 0$, il quoziente $K[x]/(f(x))$ e' una $K-$algebra di dimensione finita n. Una $K-$algebra di dimensione finita e' un dominio d'integrita' se e solo se e' un campo. Un quoziente $K[x]/(f(x))$ e' un dominio d'integrita' sse e' un campo sse $f(x)$ e' irriducibile.

Divisibilita' in un dominio d'integrita'; relazione di preordine "divide" e relative relazioni d'equivalenza e ordine parziale. Corrispondenza fra elementi ed ideali principali, dualita' rispetto alle relazioni "divide" ed "e' contenuto". Elementi irriducibili, elementi primi. Domini euclidei. Un dominio euclideo e' a ideali principali. Identita' di Bezout, forma debole. Lemma: irriducibile implica primo. Teorema di fattorizzazione unica.

Campo ordinato completo $\mathbb{R}$ dei numeri reali. Segmenti costruibili incommensurabili ed equazioni algebriche non risolubili in $\mathbb{Q}$. Problemi, definizioni e processi in geometria euclidea all'origine dell'idea di numero reale. Due definizioni equivalenti di campo ordinato. Ogni campo ordinato ha campo minimo isomorfo a $\mathbb{Q}$. Definizioni di campo ordinato completo e di campo ordinato continuo, e loro equivalenza. Un campo ordinato completo K e' archimedeo e in esso il campo minimo K_0 e' denso; gli elementi di K e le operazioni su K sono univocamente determinati, tramite l'ordine, da sottinsiemi di K_0 e operazioni in K_0. Se H e K sono due campi ordinati completi, allora H e K sono isomorfi tramite un unico isomorfismo. Costruzione di un campo ordinato completo tramite sezioni (superiori) di Dedekind. Definizione del campo ordinato $\mathbb{R}$ dei numeri reali come l'unico campo ordinato completo.

Radice di un numero reale non negativo. Polinomi di II grado. Numeri reali algebrici,

polinomio minimo; numeri reali trascendenti. Sottoanello $\mathbb{Q}[\alpha]$ e sottocampo $\mathbb{Q}(\alpha)$ generati da un $\alpha \in \mathbb{R}$, nel caso α algebrico o trascendente.

Successioni convergenti, di Cauchy, completezza; serie e prodotti infiniti. Scritture di numeri reali in una data base. Funzioni reali di variabile reale; continuita', teorema degli zeri. Radice di un numero reale non negativo.

Geometria analitica. Definizioni, costruzioni e proposizioni su grandezze, rapporti e proporzioni e i teoremi di Talete. Coordinate sulla retta; coordinate nel piano, equazioni della retta, condizione di parallelismo; sistema cartesiano ortogonale monometrico, distanza fra punti, equazione della circonferenza, condizione di ortogonalita, distanza punto-retta. Il percorso inverso. Struttura vettoriale e vettoriale euclidea sui vettori del piano, strutture affine ed euclidea su punti e vettori del piano.

Campo algebricamente chiuso $\mathbb{C}$ *dei numeri complessi.* Costruzione formale, costruzione geometrica, costruzione come quoziente $\mathbb{R}[x]/(x^2+1)$. Coniugio. Il campo complesso non e ordinato. Chiusura algebrica. Polinomi di II grado. Radici dell'unita'; radici.

Campo ottenuto per aggiunzione ad un campo $\mathbb{K}$ di una radice di un polinomio $p(x)$ irriducibile in $\mathbb{K}[x]$ (corps de rupture). Costruzione come campo $\mathbb{K}[x]/(p(x))$ con immersione $\pi : \mathbb{K} \to \mathbb{K}[x]/(p(x))$ ed elemento $\pi(x) = [x] \in \mathbb{K}[x]/(p(x))$ radice di $\pi(p)(x)$ in $\pi(\mathbb{K})[x]$. Proprieta' universale.

Estensioni di sottocampi di $\mathbb{C}$, *corrispondenza di Galois.* Estensioni di sottocampi di $\mathbb{C}$. Per un'estensione $\mathbb{F}/\mathbb{K}$. Campo $\mathbb{F}$ come $\mathbb{K}-$algebra, grado $[\mathbb{F} : \mathbb{K}]$. Elemento algebrico su $\mathbb{K}$, polinomio minimo; irriducibilita'; un criterio per la determinazione. Elemento trascendente su $\mathbb{K}$. Per ogni $\alpha \in \mathbb{F}$, omomorfismo $E : \mathbb{K}[x] \to \mathbb{F}$ di sostituzione di x in α, sua immagine $\mathrm{Im}(E) = \mathbb{K}[\alpha]$ sottoanello di $\mathbb{F}$ generato da $\mathbb{K}$ ed α, e $\mathbb{K}(\alpha)$ sottocampo di $\mathbb{F}$ generato da $\mathbb{K}$ ed α. Per α algebrico su $\mathbb{K}$ con polinomio minimo $p(x)$, si ha $\mathbb{K}[x]/(p(x)) \simeq \mathbb{K}[\alpha] = \mathbb{K}(\alpha)$; per α trascendente su $\mathbb{K}$, si ha $\mathbb{K}[x] \simeq \mathbb{K}[\alpha] \subset \mathbb{K}(\alpha)$. Caratterizzazione degli elementi α algebrici e trascendenti su $\mathbb{K}$ mediante finitezza dell'estensione $\mathbb{K}[\alpha]/\mathbb{K}$.

Per estensioni $\mathbb{F}/\mathbb{K}$, $\mathbb{F}/L$ ed $L/\mathbb{K}$, equivalenza fra finitezza della prima e simultanea finitezza delle seconde, e relazione $[\mathbb{F} : \mathbb{K}] = [\mathbb{F} : L][L : \mathbb{K}]$. Per un'estensione finita $\mathbb{F}/\mathbb{K}$, ogni elemento $\alpha \in \mathbb{F}$ e' algebrico su $\mathbb{K}$, con grado divisore di $[\mathbb{F} : \mathbb{K}]$. Per un'estensione $\mathbb{F}/\mathbb{K}$, gli elementi di $\mathbb{F}$ algebrici su $\mathbb{K}$ formano un campo, algebricamente chiuso relativamente ad $\mathbb{F}$. I numeri algebrici formano un campo algebricamente chiuso. Cenno ai numeri costruibili con riga e compasso.

$\mathbb{K}-$automorfismi di un'estensione $\mathbb{F}/\mathbb{K}$. Relazione fra le radici e i coefficienti di un polinomio, polinomi simmetrici elementari. Per un polinomio monico non costante, campo dei coefficienti, campo di spezzamento, e relativa estensione; limitazione sul grado dell'estensione in funzione del grado del polinomio. Estensioni quadratiche.

Estensioni normale come estensione finita $\mathbb{F}/\mathbb{K}$ tale che $\mathbb{K}$ sia il campo fissato dai $\mathbb{K}-$automorfismi di $\mathbb{F}$ o equivalentemente $\mathbb{F}$ sia il campo di spezzamento di un polinomio su $\mathbb{K}$. Il grado di un'estensione normale $\mathbb{F}/\mathbb{K}$ e' uguale al numero dei $\mathbb{K}-$automorfismi di $\mathbb{F}$. Gruppo di Galois di un polinomio monico non costante $f(x)$ su un campo $\mathbb{K}$ e sua immersione nel gruppo simmetrico sull'insieme delle radici di $f(x)$. Teorema fondamentale sulla corrispondenza di Galois fra il reticolo dei campi intermedi di un'estensione

normale $\mathbb{F}/\mathbb{K}$ e il reticolo dei sottogruppi del gruppo di Galois $\mathcal{G}(\mathbb{F}/\mathbb{K})$. Cenno alla caratterizzazione della risolubilita' per radicali delle equazioni algebriche.