ALGEBRA COMPUTAZIONALE

Programma d'esame – anno accademico 2003/04 [1]

Premesso che l'esame verte su tutto quanto visto a lezione e sugli esercizi ivi svolti o proposti, provo a fare un elenco dei concetti chiave la cui conoscenza è quindi irrinunciabile, affiancandolo con il corrispondente "saper fare". Va detto che alcuni argomenti sono segnalati come importanti solo in quanto forniscono il linguaggio senza il quale il resto dei contenuti è incomprensibile, altri sono "il succo del corso".
Per comodità di chi si prepara sugli appunti suddivido il materiale secondo i Capitoli degli appunti e non secondo ordine di importanza: come nelle guide turistiche, (*) o (**) vicino a un argomento indicano "merita una visita approfondita" e "assolutamente da non perdere".

Circa il come preparare l'esame tenete presente che è meglio avere in mente la struttura (ramificata) del corso e saperci ragionare che non affidarsi a una memorizzazione lineare; è indispensabile saper fornire definizioni (o enunciati di teoremi) chiare, saper esporre oralmente raccordando quel che si viene dicendo con qualcosa di scritto (ipotesi, tesi ecc. … espresse mediante linguaggio simbolico: per fare matematica è sempre utile avere a portata di mano carta e penna, eventualmente virtuali, perché ci si capisce meglio che non raccontando), saper fare qualche semplice esempio.
Se avete problemi di memoria non cercate di "imparare" le 13 dimostrazioni evidenziate: cercate di capirle, poi fate un taglia e incolla delle dimostrazioni su un foglio personale e portatelo con voi, in modo che possa servire come supporto di discussione. Idem per gli algoritmi più elaborati.
Tenete infine presente che l'esaminatore non è un registratore: interagisce con voi, in parte guidandovi e in parte facendosi guidare; qualche volta succede che sia l'esaminando a condurre il suo esaminatore su un terreno accidentato, salvo poi non sapere come trarsi d'impaccio: evitatelo!

Capitolo I - Terminologia
Sapere: definizione di anello, dominio di integrità, campo, sottoanello, ideale (ideale generato da …, ideale somma, ideale intersezione, massimale, primo). Anelli di polinomi in 1 o più indeterminate (terminologia sul grado ecc.); quale delle proprietà fin qui viste ereditano dall'anello base? Caso monovariato: algoritmo della divisione, teorema di Ruffini, legame tra polinomio e funzione nulla, algoritmo euclideo per il calcolo dell'MCD di 2 polinomi.
Saper fare: dare esempi di anelli non domini, di domini non campi, di campi finiti e non; verificare che un sottoinsieme di un anello è un ideale; usare i due algoritmi sui polinomi in una indeterminata.

Capitolo II - Fattorizzazioni
Sapere: definizione elementi unit, primi, irriducibili (loro relazioni), irriducibili associati. Definizione UFD: caratterizzazione in termini di irriducibili (solo enunciato); esistenza MCD, mcm. Definizione PID, dominio euclideo (loro relazioni); ideali primi di un PID; ideali generati da MCD e mcm in un PID; relazioni tra PID e UFD. Quale delle proprietà fin qui viste gli anelli di polinomi ereditano dall'anello base?
Saper fare: qualche esempio degli oggetti sopra definiti, magari anche di un dominio a fattorizzazione non unica.

Capitolo III - Ordinamenti sui monomi di $k[x_1,\ldots, x_n]$
Sapere: definizione ordinamento, totale, buono (e su $\mathbf{N}^n$: monoidale, monomiale); CNS perché un ordinamento monoidale sia monomiale; rappresentazione di ordinamenti attraverso matrici: quando sono monoidali e monomiali? Quando due matrici invertibili rappresentano lo stesso ordinamento?
Saper fare: esempi di ordinamenti monomiali e non; mettere in ordine alcuni monomi in base a tali ordinamenti. Saper tradurre un ordinamento noto in matrice.

[1] Evidenziati in azzurro i temi non trattati e quindi non in programma nell'anno accademico 2007/08.

Capitolo IV - Divisioni in $[x_1,\ldots, x_n]$ e teorema della base
Sapere: definizione di LT di un polinomio rispetto a un ordinamento monomiale; concetto di divisione per più divisori (**), teorema di unicità (enunciato e dimostrazione) ed esistenza (algoritmo enunciato in dettaglio). Definizione ideale monomiale, sua descrizione attraverso i monomi che contiene. Lemma di Dickson (enunciato) e conseguenze sugli ordinamenti monoidali. Ideale dei LT di un ideale, teorema della base (**) con dimostrazione. Validità della CCA sugli ideali di polinomi.
Saper fare (fissato un ordinamento monomiale): individuare il LT di un polinomio, dividere un polinomio per un insieme ordinato di polinomi; cogliere la differenza tra ideale dei LT e ideale generato dai LT dei generatori di un ideale.

Capitolo V - Basi di Gröbner (**)
Sapere: Definizione e dimostrazione di esistenza; unicità del resto nella divisione per una base di G. e caratterizzazione tramite resto; basi minimali e ridotte (*) come ottenerle. Definizione sizigia (*), sizigia omogenea; sizigie elementari come base del modulo delle sizigie di un insieme di LT (enunciati); in quali ipotesi si possono eliminare sizigie elementari da una base del modulo? Definizione riducibilità a zero modulo una base di polinomi (*): alcuni casi in cui succede (resto nullo, polinomio sizigietico con i 2 LT primi tra loro). Teorema di Caratterizzazione delle basi di Gröbner tramite i due concetti precedenti (**) (enunciato) e corollari che coinvolgono resto nullo e polinomi sizigietici (con verifica). Algoritmo ingenuo (**) (con dimostrazione). Algoritmo di Buchberger (enunciato). Possibili migliorie.
Saper fare (fissato un ordinamento monomiale): dati due polinomi, calcolare la sizigia elementare dei LT e/o il polinomio sizigietico. Dare esempi di insiemi di polinomi che formano ovviamente una base di Gröbner. Calcolare una base di Gröbner (*) rispetto a un ordinamento monomiale assegnato; ridurre una base (*). Sapere inoltre: risolvere il problema dell'appartenenza a un ideale (*); risolvere il problema della coincidenza di due ideali descritti attraverso due sistemi di generatori (*); (facoltativo) trovare un sistema di generatori per un ideale intersezione.

Capitolo VI - Soluzioni di sistemi ed ideali
Sapere: definizione di spazio affine, varietà algebrica affine, varietà definita da un ideale (*); loro proprietà (con verifica). Definizione di ideale di (un insieme o di) una varietà algebrica affine (*); loro proprietà (con verifica). Analogie e differenze tra le due mappe anche alla luce delle cose illustrate in Cap. VIII. Varietà algebriche affini come soluzioni di sistemi di equazioni algebriche: problemi di consistenza, dimensione e determinazione delle soluzioni.
Saper fare: esempi di varietà e non varietà.

Capitolo VII - Eliminando ed estendendo
Sapere: definizione di sistema equivalente, ideale (e ordinamento) di eliminazione h-esima; teorema di eliminazione (con dimostrazione: che cosa dimostra questo teorema?) (**). Problemi relativi al passo di estensione. Teorema di estensione in forma algebrica (**) (enunciato e facoltativamente dimostrazione nel caso di due incognite): casi particolari in cui si garantisce l'estensione. Definizione di proiezione h-esima; relazione tra la proiezione h-esima di una varietà e varietà dell'ideale di eliminazione h-esima (*); teorema di estensione in forma geometrica. Facoltativamente. Teoria del risultante: da quale problema nasce la matrice di Sylvester e che cosa diagnostica l'annullarsi del risultante nel caso di polinomi univariati; generalizzazione nel caso multivariato: risultante rispetto a x_1 come elemento dell'ideale di eliminazione prima dell'ideale generato dai due polinomi che evidenzia la presenza di fattori comuni contenenti x_1 e problema della particolarizzazione.
Saper fare: applicare la procedura di eliminazione successiva delle incognite con corretta scelta dell'ordine monomiale.

Capitolo VIII - Nullstellensatz (**)

Sapere: Nullstellensatz debole (**) (enunciato, dimostrazione versione in dimensione 1 e cenni di come sfruttare il teorema di estensione per provare l'induzione). Nullstellensatz di Hilbert (**) (enunciato, dimostrazione dando per buoni i lemmi, di cui si vuole l'enunciato). Definizione di ideale radicale e radicale di un ideale, con proprietà. Definizione di chiusura di Zariski di un sottoinsieme di uno spazio affine e utilizzo del Nullstellensatz forte (enunciato e dimostrazione) per mostrare il teorema di Chiusura (enunciato e dimostrazione). Restrizione della corrispondenza tra ideali e varietà a ideali radicali: conseguenze nel caso di campo algebricamente chiuso (*). Definizione varietà irriducibile; corrispondenza con gli ideali primi; corrispondenza tra punti e ideali massimali.

Saper fare: stabilire a priori se un sistema di equazioni algebriche è risolubile; stabilire se un polinomio appartiene al radicale di un ideale.