Università degli studi di Trieste
Corso di Studi in Matematica

Algebra 2 (9 cfu)

docente: **prof. Alessandro Logar**

anno accademico: 2013-2014

1 Richiami/premesse

Richiami su gruppi, anelli, campi; omomorfismi, nucleo, immagine. Sottogruppi, sottogruppi normali, gruppo quoziente, teoremi di omomorfismo, teorema del doppio quoziente, gruppi ciclici. Ideali, anelli quoziente, ideali primi, ideali massimali; elementi invertibili e divisori dello zero in un anello; domini di integrità; l'anello degli interi, i suoi ideali e i suoi quozienti ($\mathbb{Z}$ e $\mathbb{Z}_m$). Piccolo teorema di Fermat; teorema cinese del resto in $\mathbb{Z}$, divisione tra interi, algoritmo di Euclide e identità di Bezout.
Approfondimento sugli anelli: ideali di un anello principali e finitamente generati, ideali generati da un sottoinsieme dell'anello; caratteristica di un anello, ogni anello contiene (una copia isomorfa di) $\mathbb{Z}$ o di $\mathbb{Z}_m$. La caratteristica di un dominio d'integrità o è 0 o è un numero primo; in un anello di caratteristica p (con p primo) vale: $(a+b)^p = a^p + b^p$.

Argomenti tratti da: [3], [1], [4].

2 Domini a fattorizzazione unica

Elementi primi e irriducibili in un dominio d'integrità. Elementi associati. Un elemento $p \in A$ è primo se e solo se l'ideale (p) è primo. Ogni elemento primo è irriducibile. Definizione di massimo comun divisore in un dominio (se $a, b \in A$, d è un massimo comun divisore se $d|a$, $d|b$ e, se $\delta \in A$ è un altro elemento che divide sia a sia b, allora $\delta|d$. Due massimi comun divisori di una coppia (a, b) di elementi di A sono associati. Domini a fattorizzazione unica (UFD). Se in un dominio ogni elemento (non nullo e non invertibile) si scrive come prodotto di elementi irriducibili, allora sono equivalenti le seguenti tre affermazioni: (1) la fattorizzazione è essenzialmente unica (cioè il dominio è un UFD); (2) ogni irriducibile è primo; (3) esiste il massimo comun divisore di ogni coppia di elementi di A. $\mathbb{Z}$ è un UFD.

Argomenti tratti da: [2], [4].

3 Polinomi in una indeterminata

Costruzione dell'anello dei polinomi in una indeterminata (a coefficienti in un anello), grado di un polinomio. Termine/coefficiente direttivo di un polinomio, termine noto, polinomio monico. Principio di identità tra polinomi. L'anello dei polinomi costruito su un dominio d'integrità è, a sua volta, un dominio d'integrità. Un omomorfismo ϕ tra due anelli si estende in unico modo in un omomorfismo $\psi : A[x] \longrightarrow B[x]$ tale che $\psi(x) = x$. Omomorfismo di valutazione ($f(x) \mapsto f(a)$). Dato un omomorfismo di anelli $\phi : A \longrightarrow B$ e dato un elemento $b \in B$, esiste un unico omomorfismo $\psi : A[x] \longrightarrow B$ che estende ϕ e tale che $\psi(x) = b$.
Divisione tra polinomi. Anello dei polinomi a coefficienti in un campo; polinomi riducibili e irriducibili, algoritmo della divisione. Teorema di Ruffini. Radici di un polinomio. Teorema di D'Alambert (un polinomio di grado n a coefficienti in un campo ha al massimo n radici). Se un campo è infinito allora due polinomi f e g sono uguali se e solo se $f(a) = g(a)$ per ogni elemento a del campo.
L'anello dei polinomi $K[x]$ con K campo: il massimo comun divisore (e minimo comune multiplo) di polinomi. Algoritmo di Euclide e l'identità di Bezout per polinomi. In $K[x]$ si può definire il massimo comun divisore (come in $\mathbb{Z}$, usando l'algoritmo di Euclide). Imponendo al mcd di essere monico, è unico. $K[x]$ è un UFD. L'anello dei polinomi $K[x]$ (K campo) è un dominio ad ideali principali.

Argomenti tratti da: [2], [4], [1].

4 Fattorizzazione di polinomi, parte I

Polinomi irriducibili in $K[x]$ (K campo). Campi algebricamente chiusi. Teorema fondamentale del'algebra: il campo $\mathbb{C}$ dei numeri complessi è algebricamente chiuso (breve cenno della dimostrazione), In $\mathbb{R}$ i polinomi irriducibili o sono di grado 1, o sono di grado 2 e hanno il discriminante negativo.
Derivata di un polinomio. Se la derivata di un polinomio $f \in K[x]$ (K campo) vale 0 allora o il polinomio è una costante o, se la caratteristica di K è p, allora è della forma g^p, dove g è un opportuno polinomio di $K[x]$. Se un polinomio f di $K[x]$ ha fattori multipli, allora il massimo comun divisore tra f e la sua derivata è diverso da 1. Vale anche il viceversa, purché il campo sia di caratteristica 0 o sia finito. Definizione di campo perfetto. Isomorfismo di Frobenius.

Argomenti tratti da: [1], [6].

5 Fattorizzazione di polinomi, parte II

Polinomi di $\mathbb{Q}[x]$ e di $\mathbb{Z}[x]$. Definizione di polinomio primitivo di $\mathbb{Q}[x]$. Il prodotto di polinomi primitivi è primitivo. Lemma di Gauss. Fattorizzazione di polinomi in $\mathbb{Z}[x]$ e in $\mathbb{Q}[x]$. Ricerca delle radici razionali di un polinomio in $\mathbb{Z}[x]$. Criterio di irriducibilità di Eisenstein. In $\mathbb{Q}[x]$ e in $\mathbb{Z}[x]$ ci sono infiniti polinomi irriducibili in ogni grado.
Teorema cinese del resto (in $\mathbb{Z}$, in $\mathbb{Z}[x]$ e in un anello qualunque).
Fattorizzazione di polinomi in $\mathbb{Z}[x]$: il metodo di Schubert (Kronecker). La fattorizzazione di polinomi in $\mathbb{Z}_p[x]$: il metodo di Berlekamp (i 3 teoremi di Berlekamp). Fattorizzazione di polinomi in $\mathbb{Z}[x]$ usando fattorizzazioni in $\mathbb{Z}_p[x]$. Cenno al metodo di sollevamento di Hensel.

Argomenti tratti da: [1].

6 Polinomi in più variabili

La costruzione dell'anello dei polinomi in più variabili, grado globale, grado relativo ad una variabile, definizione di monomi, termini. Principio di identità tra polinomi. Ogni polinomio è somma finita di monomi; polinomi omogenei, ogni polinomio è somma finita di polinomi omogenei. Se A è un dominio di integrità, allora lo è anche $A[x_1, \ldots, x_n]$, se A è un UFD, allora lo è anche $A[x_1, \ldots, x_n]$ (senza dimostrazione). Estensione di un omomorfismo $\phi : A \longrightarrow B$ ad un omomorfismo $\psi : A[x_1, \ldots, x_n] \longrightarrow B$ tale che $\phi(x_i) = b_i$ (dove $b_1, \ldots, b_n$ sono n elementi fissati in B).
L'anello $K[x_1, \ldots, x_n]$ (con K campo) è uno spazio vettoriale su K di dimensione infinita (una base è costituita dall'insieme dei termini). Esempi di ideali in $K[x_1, \ldots, x_n]$: ideali non principali, ideali primi, ideali massimali; gli ideali della forma $(x_1 - a_1, \ldots, x_n - a_n)$ (con $a_i \in K$) sono tutti massimali.

Argomenti tratti da: [4].

7 Campi

Costruzione del campo dei quozienti $Q(A)$ di un dominio A. Proprietà universale di $Q(A)$.
Estensione di campi: $K \subseteq L$ (denotata anche con $L : K$). Dati $L : K$ e $b_1, \ldots, b_n \in L$, definizione del campo $K(b_1, \ldots, b_n)$, cioè del più piccolo campo che contiene K e $b_1, \ldots, b_n$. Vale: $K(b_1, \ldots, b_n) = Q\left(K[b_1, \ldots, b_n]\right)$ (dove $K[b_1, \ldots, b_n]$ indica il più piccolo sottoanello di L che contiene K e $b_1, \ldots, b_n$). Estensioni semplici. Elementi algebrici e trascendenti. Cenno

alla tascendenza di e e π su $\mathbb{Q}$. Polinomio minimo di un elemento algebrico. Se $L : K$ è un'estensione di campi e se $a \in L$ è algebrico su K, allora $K[a] = K[x]/(m)$, dove m è il polinomio minimo di a su K. Grado di un'estensione di campi. Legge della torre, legge della torre generalizzata. Dato un polinomio $f \in K[x]$ (con K campo), esiste un ampliamento di K che contiene uno zero di f. Campo di riducibilità completa di un polinomio. Il campo dei complessi $\mathbb{C}$ ottenuto come il quoziente $\mathbb{R}/(x^2 + 1)$.
Costruzioni con riga e compasso. Teoremi di Wantzel: con riga e compasso non si può duplicare il cubo; l'angolo $\pi/3$ non può essere trisecato con riga e compasso.

Argomenti tratti da: [6], [2].

8 Campi finiti

Un campo finito (di caratteristica p) è uno spazio vettoriale su $\mathbb{Z}_p$, quindi la cardinalità di un campo finito è sempre la potenza di un numero primo. Teorema dell'elemento primitivo: se K è un campo finito, allora $(K \setminus \{0\}, \cdot)$ è un gruppo ciclico. Un campo finito è della forma: $\mathbb{Z}_p[x]/(q)$ con q polinomio irriducibile. Polinomi irriducibili di $\mathbb{Z}_p[x]$. Il polinomio $x^{p^n} - x$ è il prodotto di tutti i polinomi irriducibili di $\mathbb{Z}_p[x]$ di grado d, con $d|n$. Funzione di Moebius. Calcolo del numero di polinomi irriducibili di $\mathbb{Z}_p[x]$. (formula di inversione di Moebius). Tutti i campi finiti dello stesso ordine sono isomorfi; dato p numero primo ed n, numero naturale, esiste sempre un campo con p^n elementi (e, per quanto detto, è unico). Tale campo si indica con $\mathrm{GF}(p, n)$ e si chiama campo di Galois.

Argomenti tratti da: [1].

9 Calcolo simbolico

Presentazione del programma di calcolo simbolico Sage.

Argomenti tratti da: [5].

Riferimenti bibliografici

[1] Lindsay N. Childs, *A concrete introduction to higer algebra*, Springer, I edizione (1990) e III edizione (2009);

[2] Stefania Gabelli, *Teoria delle equazioni e teoria di Galois*, Springer (2008);

[3] Israel N. Herstein, *Algebra*, Roma, Editori Riuniti (1992).

[4] Nathan Jacobson, *Basic Algebra*, San Francisco: W.H. Freeman (1974);

[5] William Stein, *Elementary number theory: Primes, Congruences, and Secrets*, Springer, 2008 - scaricabile gratuitamente da:
`http://wstein.org/ent/ent.pdf`

[6] Ian Stewart, *Galois theory*, Chapman & Hall/Crc Mathematics (2004);