

Programma del corso

Complementi sui gruppi

Sottogruppo generato da un sottoinsieme: definizione, caratterizzazione, caso dei gruppi simmetrici ed alterni. Secondo e terzo teorema di isomorfismo per gruppi. Gruppi risolubili: definizione, gruppi derivati, caratterizzazione mediante le catene normali, risolubilità di sottogruppi e gruppi quoziensi, caso dei gruppi simmetrici, teorema di Galois-Jordan*, risolubilità dei p -gruppi, teoremi di Burnside* e di Feit-Thompson.

Complementi su polinomi e campi

Unicità del campo di spezzamento, teoremi di estensione degli isomorfismi di campo: forma debole, forma forte*. Polinomi separabili, estensioni separabili, campi perfetti. Teorema dell'elemento primitivo. Immersioni di un'estensione separabile in una chiusura algebrica. Lemma di Dedekind. Estensioni algebriche semplici e finitezza dei campi intermedi. Teorema di Lüroth*. Polinomi simmetrici e polinomi simmetrici elementari, polinomi simmetrizzati per somma e per prodotto, funzioni razionali simmetriche, formule di Viète. Risultante di due polinomi: espressioni mediante la matrice di Sylvester e mediante le radici*. Discriminante di un polinomio: definizione tramite il risultante, calcolo mediante la matrice di Vandermonde, relazione con la molteplicità delle radici (caso particolare dei polinomi reali quadratici e cubici). Polinomi ciclotomici: definizione, formula ricorsiva, irriducibilità*, polinomi ciclotomici di ordine primo, applicazione alla dimostrazione del teorema di Wedderburn sui corpi finiti*.

Teoria di Galois

Teoria di Galois

Teorema Fondamentale dell'Algebra*. Gruppo di Galois del composto di un'estensione galoisiana e di un'estensione algebrica*. Gruppo di Galois di un polinomio, suo studio per i polinomi di grado 2,3,4*, per i polinomi ciclotomici, per le equazioni binomie e l'equazione generale di grado n . Formule risolutive delle equazioni algebriche di grado 2, 3, 4, risolvente cubica di Ferrari e sua variante*. Estensioni radicali: definizione e caratterizzazione*. Criterio di risolubilità per radicali. Segmenti costruibili con riga e compasso e numeri reali costruibili. Trascendenza di π secondo il teorema di Lindemann. Costruzioni impossibili. Numeri complessi costruibili: definizione e caratterizzazione*. Criterio di Gauss per la costruibilità di un poligono regolare.

Teoria algebrica dei numeri

Generalità sui moduli sugli anelli commutativi unitari: definizione, sottomodulo generato da un sottoinsieme, moduli finitamente generati, moduli liberi e non liberi, rango di un modulo libero, moduli liberi su \mathbf{Z} e loro sottomoduli*, omomorfismi di moduli, moduli quoziante. Anelli e moduli noetheriani: definizioni equivalenti, teorema della base di Hilbert*, quozianti, sottomoduli e somme dirette finite di moduli noetheriani, moduli noetheriani su un anello noetheriano. Dimostrazione che ogni ideale di un anello commutativo unitario è contenuto in un ideale massimale*. Elementi interi ed estensioni intere: definizione, caratterizzazione, interi algebrici (caratterizzazione, relazione con i numeri algebrici), criterio sufficiente per le estensioni intere, transitività delle estensioni intere, chiusure intere (dimostrazione di Milne che la chiusura intera è un anello*), anelli integralmente chiusi, il caso di \mathbf{Z} (e, più in generale, di un UFD). L'anello degli interi DK di un campo numerico K : teorema di caratterizzazione nel caso di un campo quadratico, DK come dominio di Dedekind. Relazione tra PID e UFD: caso generale e caso dei domini di Dedekind. Ideali frazionari. Relazione di divisibilità tra ideali. Fattorizzazione e gruppo moltiplicativo degli ideali non nulli di un dominio di Dedekind: criterio di fattorizzazione di Kummer*, numeri interi che sono primi in DK . Norma, traccia e caratteristica di un elemento in un'estensione finita di campi. Norma di un ideale di D : definizione, confronto con le norme dei suoi elementi, proprietà moltiplicativa*. Gruppo delle classi di ideali: due definizioni equivalenti, relazione con la proprietà di PID, numero delle classi di ideali ed applicazioni alla risolubilità di equazioni diofantee. Caratterizzazione dei PID mediante la norma di Hasse-Dedekind. Criterio necessario per i domini euclidei. Esempio di un PID che non è un dominio euclideo. Residui quadratici modulo un primo: definizione, criterio di Eulero, Lemma di Gauss, legge di reciprocità quadratica.

Metodi di insegnamento:

Lezioni ed esercitazioni in aula.

Supporti alla didattica:

Sono disponibili in rete le dispense complete del corso:

http://www.dm.uniba.it/~barile/Rete2/indice_dispense.htm

Controllo dell'apprendimento e modalità d'esame:

Prova orale.

Testi di riferimento principali:

[A] R. B. Ash, *A Course in Algebraic Number Theory*,

<https://faculty.math.illinois.edu/~r-ash/ANT.html>

[A2] R. B. Ash, *Abstract Algebra, The Basic Graduate Year*

<https://faculty.math.illinois.edu/~r-ash/Algebra.html>

[AM] M. F. Atiyah, I.G. Macdonald, *Introduzione all'algebra commutativa*, trad. di P. Maroscia, Feltrinelli, Milano, 1981.

[B] M. Baker, *Algebraic Number Theory*,

<http://people.math.gatech.edu/~mbaker/pdf/ANTBook.pdf>

[CM] A. Caranti, S. Mattarei, *Introduzione alla Teoria di Galois*,

<http://www.science.unitn.it/~caranti/Didattica/Galois/2005-06/Note/Galois.pdf>

[DF] D. S. Dummit, R. M. Foote, *Abstract Algebra*, Wiley, New York, 1999.

[FdG] S. Franciosi, F. de Giovanni, *Elementi di Algebra*, Aracne, Roma, 1992.

[Gr] J. Greene, "Principal Ideal Domains are almost Euclidean", *American Mathematical Monthly*, **104** (1997), pagg. 154-156.

[G] P. Grillet, *Algebra*, John Wiley & Sons, New York, 1999.

[Ha] H. Hasse, "Über eindeutige Zerlegung in Primelemente oder in Primhauptideale in Integritätsbereichen", *Journal für die Reine und Angewandte Mathematik*, **159** (1928), pagg. 3-12.

[H] I. N. Herstein, *Algebra*, Editori Riuniti, Roma, 1994.

[I] I. M. Isaacs, *Algebra. A Graduate Course*, Brooks/Cole, Pacific Grove, 1994.

[Mi] J. S. Milne, *Algebraic Number Theory*,

<http://www.jmilne.org/math/CourseNotes/ANT.pdf>

- [Mo] P. Morandi, *Field and Galois Theory*, Springer, New York, 1996.
- [PC] G. M. Piacentini Cattaneo, *Algebra: un approccio algoritmico*, Decibel-Zanichelli, Bologna, 2001.
- [Ri] P. Ribenboim, *13 Lectures on Fermat's Last Theorem*, Springer, New York, 1979.
- [Ro] J. Rotman, *Galois Theory*, Springer, New York, 1990