AL4 Numeri Algebrici
A.A. 2007/2008
Prof. Marco Fontana

1. Anelli di interi e campi quadratici

Interi di Gauss: norma, coniugio, algoritmo euclideo, elementi primi, elementi invertibili e relazione di associazione.

Campi di numeri quadratici. Discriminante. Coniugio, norma e traccia. Prime proprietà. Basi e discriminante.

Anello di interi in un campo quadratico: polinomio minimo quadratico, relazione con norma e traccia. Varie costruzioni equivalenti dell'anello degli interi quadratici di $\mathbb{Q}(\sqrt{d})$. L'anello degli interi quadratici è noetheriano.

Elementi invertibili ed elementi irriducibili e primi in un anello di interi quadratici. In un anello di interi quadratici ogni elemento non zero e non invertibile si può fattorizzare nel prodotto finito di elementi irriducibili.

In generale un anello di interi quadratici non è fattoriale, non possiede MCD, non soddisfa le conclusioni del lemma di Euclide. L'anello degli interi quadratici è un dominio euclideo per d = -11, -7, -3, -1, 2, 3, 5, 13. Un dominio di interi quadratici se è un UFD è un PID. Nel caso di un dominio di interi quadratici le nozioni di PID, UFD, dominio bézoutiano, dominio pseudo-bézoutiano (o MCD-dominio) coincidono (cenni).

Cenni alla problematica generale relativa allo studio dei domini di interi quadratici che sono euclidei (rispetto al modulo della norma) oppure fattoriali (cenni sulla congettura di Gauss).

Elementi invertibili dell'anello degli interi di un campo quadratico. Unità fondamentale. Relazione con le soluzioni dell'equazione di Pell-Fermat (cenni). Anelli di interi in campi di numeri algebrici e Teorema delle unità di Dirichlet (cenni).

2. Anelli di interi in campi di numeri algebrici

Estensioni di campi. Estensioni algebriche e finite. Grado di un'estensione. Polinomio minimo. Teorema dell'elemento primitivo.

Polinomi simmetrici e polinomi simmetrici elementari. Teorema fondamentale.

$\mathbb{Z}$-moduli liberi e rango. Sottomoduli di $\mathbb{Z}$-moduli liberi di rango finito. Teorema fondamentale. Matrici di cambiamento di base di moduli liberi. Ordine dello $\mathbb{Z}$-modulo quoziente di uno $\mathbb{Z}$-modulo libero di rango finito modulo un suo sottomodulo dello stesso rango.

Dipendenza integrale, anelli integralmente chiusi. Interi algebrici. Caso dei campi quadratici. Polinomi ciclotomici. Campi ciclotomici. Interi ciclotomici.

Coniugati e discriminante. Discriminante di una base di un campo di numeri algebrici.

Basi intere. Discriminante di un campo di numeri. Teorema fondamentale di esistenza di basi intere. Esempi di calcolo di basi intere.

Norme e tracce. Discriminante e norma del polinomio minimo di un'estensione algebrica semplice. Discriminante e traccia.

Ideali ed ideali frazionari. Teorema di fattorizzazione unica di ideali frazionari di un anello di interi algebrici. Domini di Dedekind. Assiomi di Noether. Norma di un ideale. Principali proprietà della norma di un ideale. Ogni anello di interi algebrici è un dominio di Dedekind. Esempi di calcolo della fattorizzazione unica in prodotto di potenze di ideali primi di un ideale non nullo in un dominio di Dedekind. Ogni ideale di un anello di interi algebrici può essere generato da al più due elementi.

Rappresentazione geometrica dei campi di numeri algebrici. Tori e domini fondamentali. Teorema di Minkowski.

Gruppo delle classi. Teorema di finitezza del numero delle classi. PID e numero delle classi. Esempi di calcolo del numero delle classi. Finitezza del gruppo delle classi di un anello di interi algebrici, teorema di Dirichlet.

Testi consigliati

[1] W.W. Adams - L.J. Goldstein, *An introduction to the theory of numbers*. Prentice-Hall, (1976).
[2] Z.I. Borevich - I.R. Shafarevich, *Number Theory*. Academic Press, (1964).
[3] H. Cohn, *A classical invitation to algebraic numbers and class fields*. Springer, (1978).
[4] G.H. Hardy- E.M. Wright, *An introduction to the theory of numbers*. Oxford Univ. Press, (1960; 4a Ed.).
[5] K.F. Ireland - M. I. Rosen, *A classical introduction to modern number theory*. Springer, (1982).
[6] H. E. Rose, *A course in number theory*. Oxford Science Publ., (1988).
[7] H. M. Stark, *An introduction to number theory*. MIT Press, (1987).
[8] I.N. Stewart - D.O. Tall, *Algebraic number theory*. Chapman-Hall, (1987).

Bibliografia supplementare

[9] C.F. Gauss, *Disquisitiones Arithmeticae (trad. Ingl.)*. Yale Univ. Press, (1966).
[10] I. Niven - H.S. Zuckerman, *An introductionto the theory of numbers*. J. Wiley, (1972; 3a Ed.).
[11] P. Samuel, *Théorie algébrique des nombres*. Hermann, (1967).
[12] J.-P. Serre, *Cours d'arithmétique*. PUF, (1970).
[13] A. Weil, *Number theory: an approach through history*. Birkauser, (1983).

Modalità d'esame

- valutazione in itinere ("esoneri")		■ SI	□ NO
- esame finale	scritto	■ SI	□ NO
	orale	■ SI	□ NO
- altre prove di valutazione del profitto (meglio descritte sotto)		■ SI	□ NO

Gli studenti che hanno sostenuto con esito positivo, nel corso del semestre, le prove di valutazione parziale (seminari e prova scritta) accedono direttamente al colloquio di verbalizzazione del voto proposto dal docente, da effettuarsi durante la I Sessione di esame (Appello **A** o **B**).

Per tutti gli studenti che non si avvalgono della possibilità della valutazione del profitto durante il corso, l'esame finale consiste in una prova orale o/e scritta (comprendente anche domande di tipo teorico).

Gli studenti che non hanno frequentato il corso debbono prenotarsi almeno 10 giorni prima dell'appello d'esame, contattando il docente nell'orario di ricevimento.