

AL5 Istituzioni di Algebra Superiore, 2^o Modulo

A.A. 2000/2001

Prof. Marco Fontana

Argomenti di Teoria Algebrica dei Numeri

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 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).

Equazione diofantea di Pell-Fermat: soluzione fondamentale, teorema di determinazione delle soluzioni, algoritmo di calcolo della soluzione fondamentale.

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

2. Moduli (reti) in campi quadratici e forme quadratiche

Basi e discriminante in un campo di numeri quadratici. Ogni ideale di un anello di interi quadratici può essere generato da al più due elementi. \mathbb{Z} -moduli liberi. Moduli o reti in un campo di numeri quadratici. Discriminante di una rete, base di una rete. Anello dei coefficienti di una rete. Conduttori: prime proprietà. Ideali frazionari e reti in un campo di numeri quadratici. Ordini. Caratterizzazione degli ordini in un campo di numeri quadratici. Prime proprietà di tali anelli. Cenno sugli elementi invertibili e relazione con gli elementi invertibili dell'anello degli interi quadratici. Basi speciali di una rete.

Determinazione dell'anello dei coefficienti di una rete espressa tramite una base speciale. Anello-quotiente di una rete intera nel suo anello dei coefficienti. Norma di una rete e cardinalità dell'anello-quotiente. Rete coniugata, norma di una rete. Prime proprietà. Prodotto di reti: prime proprietà. Teoria della divisibilità per reti: reti irriducibili, MCD di due reti (esistenza ed unicità), lemma di Euclide per reti.

Teorema di fattorizzazione unica di reti intere in un ordine. Domini di Dedekind. Ogni anello di interi quadratici è un dominio di Dedekind. Decomposizione dell'ideale principale generato da un numero primo in un anello di interi quadratici. Primi inerti, decomposti, ramificati: i Cenni al caso di anelli di interi algebrici. Gruppo delle classi di un ordine. Teorema di finitezza del numero delle classi. PID e numero delle classi. Esempi di calcolo del numero delle classi. Teorema di Minkowski (cenno). Cenno sulla 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 introduction to 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*. Birkhäuser, (1983).

MODALITÀ D'ESAME

- valutazione in itinere (“esoneri”)		<input checked="" type="checkbox"/> SI	<input type="checkbox"/> NO
- esame finale	scritto	<input checked="" type="checkbox"/> SI	<input type="checkbox"/> NO
	orale	<input type="checkbox"/> SI	<input checked="" type="checkbox"/> NO
- altre prove di valutazione del profitto (meglio descritte sotto)		<input checked="" type="checkbox"/> SI	<input type="checkbox"/> NO

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

Per tutti gli studenti che non si avvalgono della possibilità della valutazione del profitto durante il corso, l’esame finale consiste in una prova 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.