Aoi

155

Fabio Stumbo

COMPUTER ALGEBRA

www.aracneeditrice.it
info@aracneeditrice.it

via Raffaele Garofalo, 133/A–B
00173 Roma
(06) 93781065

ISBN 978–88–548–3465–1

I edizione: settembre 2010

Indice

Introduzione **vii**

1 Gruppi **1**
1.1 Nozioni di base 1

2 Anelli **5**
2.1 Anelli 5
2.2 Ideali 11
2.3 Ideali principali e fattorizzazione unica 12
2.4 Anelli euclidei 14
2.5 L'algoritmo euclideo e l'identità di Bézout 16
2.6 Congruenze e classi di congruenza 22
2.7 Operazioni con le congruenze 24
2.8 Equazioni e sistemi di congruenze 24
2.9 Il Teorema Cinese del Resto 28

3 Esempi fondamentali **31**
3.1 Numeri interi e sistemi di numerazione posizionali 31
3.1.1 Notazione posizionale 32
3.1.2 Operazioni elementari 36
3.1.3 Cambio di base 44
3.2 Numeri interi e congruenze 47
3.2.1 Congruenze 47
3.2.2 Classi di congruenze 49
3.2.3 Il Teorema di Eulero–Fermat 50
3.2.4 Potenze "grandi" di una classe di congruenza 51
3.2.5 Applicazioni: successioni di numeri pseudocasuali 54
3.2.6 Applicazioni: campi con p elementi. 58
3.3 Polinomi a coefficienti in un campo 60
3.3.1 L'anello dei polinomi 60
3.3.2 La divisione tra polinomi 62
3.3.3 Conseguenze della divisione tra polinomi 67
3.3.4 L'anello quoziente 68
3.3.5 La derivata di un polinomio 69
3.3.6 Il lemma di Gauss 72

4 Campi **77**
4.1 Campi finiti 77
4.2 Elementi primitivi 78
4.3 Costruzione di campi finiti 79
4.3.1 Rappresentazione degli elementi di un campo finito 79
4.3.2 Un esempio: $GF(8)$ 80
4.3.3 Un esempio importante: $GF(256)$ 82
4.4 Approfondimento: struttura dei campi finiti 85

5 Cenni di complessità computazionale **89**
5.1 La notazione O-grande ed o-piccolo 89
5.2 Lunghezza dei numeri 91
5.3 Tempo di esecuzione di un algoritmo 92
5.3.1 Operazioni elementari 93
5.3.2 Tempo di esecuzione delle operazioni aritmetiche 94
5.3.3 Tempo polinomiale e tempo esponenziale 96
5.4 Esempi importanti 98
5.4.1 Il cambio di base 98
5.4.2 Il calcolo di $n!$ 98
5.4.3 L'algoritmo "square and multiply" 98
5.4.4 L'algoritmo euclideo 99

6 Crittografia **107**
6.1 Concetti fondamentali 107
6.1.1 Cifrari 107
6.1.2 Sicurezza di un cifrario 109
6.2 Cenni storici 110
6.3 Cifrari monoalfabetici 113
6.3.1 Cifrari storici 113
6.3.2 Permutazioni e sostituzioni 115
6.4 Cifrari polialfabetici simmetrici 116
6.4.1 Cifrario di Vigenère 118
6.4.2 Cifrario di Hill 119
6.4.3 Cifrario DES 121
6.4.4 Cifrario AES 124
6.4.5 Il cifrario perfetto: OneTimePad 136
6.5 Cifrari polialfabetici asimmetrici 139
6.5.1 Cifrario RSA 140
6.5.2 Cifrario ElGamal 142
6.6 Funzioni di hash 144
6.6.1 SHA–1 144
6.7 Firma digitale 148
6.7.1 DSA 150

7 Codici autocorrettivi **155**
7.1 Codici di Hamming 156
7.2 Codici BCH 158

8 Fattorizzazione di numeri **161**
8.1 Test di primalità 162
8.1.1 Il crivello di Eratostene 162
8.1.2 Algoritmo di Miller–Rabin 163
8.1.3 Algoritmo AKS 165
8.2 Algoritmi di fattorizzazione 167
8.2.1 Algoritmo ρ di Pollard 168
8.2.2 Algoritmo $p-1$ di Pollard 172

9 Fattorizzazione di polinomi in $\mathbb{Q}[x]$ **175**
9.1 Riduzione del problema in $\mathbb{Z}[x]$ 176
9.2 Riduzione del problema in $\mathbb{Z}_p[x]$ 177
9.3 Fattorizzazione in $\mathbb{Z}_p[x]$: l'algoritmo di Berlekamp 178
9.4 Fattorizzazione in $\mathbb{Z}[x]$: sollevamento henseliano 182
9.4.1 Fattorizzazioni in $\mathbb{Z}_M[x]$ e fattorizzazioni in $\mathbb{Z}[x]$ 183
9.4.2 Sollevamento di una fattorizzazione da $\mathbb{Z}_p[x]$ a $\mathbb{Z}_{p^{2^m}}[x]$ per ogni $m \in \mathbb{Z}$ 185
9.5 Esempi 190

Bibliografia **197**

Indice delle tabelle **197**

Indice delle figure **199**

Indice degli algoritmi **200**

Indice dei cifrari **201**

Indice analitico **202**

Introduzione

Queste note nascono come le dispense del corso di *Computer Algebra* del Corso di Laurea Specialistica in Informatica dell'Università di Ferrara. Esse coprono tutti gli argomenti affrontati nel corso, aggiungendo quanto necessario per rendere la trattazione organica ed autosufficiente.

Il fatto che nel Corso di Laurea in Informatica non vengano mai affrontati argomenti di carattere algebrico richiede che tutte le nozioni elementari di teoria degli anelli siano introdotte agli studenti: ciò, naturalmente, riduce lo spazio per gli argomenti più caratterizzanti del corso; per esempio, non viene neanche sfiorato un argomento fondamentale nella Computer Algebra come le basi di Groebner.

Anche la trattazione di altri argomenti risente del tempo speso per introdurre le necessarie nozioni algebriche, nonché del fatto che si tratta di un corso introduttivo; nel mostrare alcune applicazioni introduciamo la problematica di fondo, mostriamo una o più soluzioni al problema, ma non ci addentriamo in ulteriori approfondimenti: pur fornendo qualche nozione di complessità computazionale, le generalizzazioni e le ottimizzazioni non vengono affrontate, ma lasciate a corsi più avanzati. Ciò lo si può vedere per esempio nel capitolo 7 dedicato ai codici autocorrettivi ed è, più in generale, la linea guida del corso.

Naturalmente nel libro le nozioni, in particolare quelle matematiche, vengono trattate in modo più formale di quanto non fatto a lezione, pur restando piuttosto lontani dal formalismo necessario in un corso di laurea in Matematica: diciamo che per lo studente proveniente da matematica i primi due capitoli possono essere considerati come un pro memoria di veloce consultazione. Per contro, lo studente proveniente da informatica troverà maggior aiuto nel terzo e quarto capitolo, dove i primi due vengono esemplificati ai casi di particolare interesse per il corso. Da questo punto di vista, c'è una certa ridondanza tra i primi capitoli, però è intenzionale nonché, speriamo, utile per gli studenti.

Nonostante l'attenzione posta nella stesura delle note e le varie riletture, sicuramente il testo conterrà errori distribuiti in modo casuale qua e là per tenere sveglia l'attenzione del lettore...

Chiunque, trovandone uno, lo segnalerà con una e-mail all'indirizzo di posta elettronica `f.stumbo@unife.it`, riceverà un sentito ringraziamento da parte dell'autore.

Ferrara, 14 luglio 2009

Fabio Stumbo

Capitolo 1

Gruppi

L'unica nozione di teoria dei gruppi necessaria ai nostri scopi è quella di ordine di un elemento e le sue proprietà più elementari.

1.1 Nozioni di base

DEFINIZIONE 1.1.1. *Un* ***gruppo*** *è un insieme G con un'operazione di composizione interna*

$$\begin{array}{ccc} G \times G & \longrightarrow & G \\ (g,h) & \longmapsto & gh \end{array}$$

ed un elemento 1_G tali che valgano le proprietà

1. ***Proprietà associativa:*** $\forall g,h,k \in G, \quad g(hk) = (gh)k.$
2. ***Elemento neutro:*** $\forall g \in G \quad 1_G g = g 1_G = g.$
3. ***Inverso:*** $\forall g \in G \ \exists g^{-1} \in G \ \ t.c.\ gg^{-1} = g^{-1}g = 1_G.$

Se vale anche la

4. ***Proprietà commutativa:*** $\forall g,h \in G, \quad gh = hg,$

si dice che il gruppo è ***commutativo*** *od anche* ***abeliano,*** *dal matematico norvegese N. Abel.*

DEFINIZIONE 1.1.2. *Se G è un gruppo e $g \in G$, definiamo l'****ordine*** *di g come*

$$o(g) = \min\{i \in \mathbb{N} \ \ t.c.\ 0 < i \ e\ g^i = 1_G\}.$$

Se per ogni $i > 0$ si ha che $g^i \neq 1_G$, si dice che l'ordine di g è ∞.

DEFINIZIONE 1.1.3. *Sia G un gruppo, $g \in G$ e $n \in \mathbb{Z}$. L'elemento g^n di G è definito come*

$$g^n = \begin{cases} \underbrace{g \cdot g \cdot \ldots \cdot g}_{n\ volte} & se\ n > 0 \\ 1 & se\ n = 0 \\ (g^{-1})^{-n} & se\ n < 0 \end{cases}$$

OSSERVAZIONE 1.1.4. In generale, se si hanno due elementi g_1, g_2 di un gruppo G, *non* è vero che $(g_1g_2)^n = g_1^n g_2^n$. Infatti, per definizione,

$$(g_1g_2)^n = g_1g_2g_1g_2g_1g_2 \dots g_1g_2$$

e non siamo autorizzati a commutare gli elementi.
Naturalmente, ciò è vero se il gruppo è abeliano.

Le proprietà che ci interessano dell'ordine di un elemento sono tutte riassunte nel

TEOREMA 1.1.5. *Sia G un gruppo finito, $n = |G|$, $g, g_1, g_2 \in G$.*

i. $o(g) < \infty$.

ii. *Se* $0 \leq r < s < o(g)$, *allora* $g^r \neq g^s$.

iii. $o(g)|n$.

iv. $g^m = 1 \Leftrightarrow o(g)|m$.

v. $o(g^{-1}) = o(g)$.

vi. $g_1g_2 = g_2g_1$ *e* $\mathrm{MCD}(o(g_1), o(g_2)) = 1 \Rightarrow o(g_1g_2) = o(g_1)o(g_2)$.

Dimostrazione. i. Consideriamo l'insieme

$$X = \{1_G, g, g^2, g^3, \dots, g^{n-1}, g^n\}.$$

Esso ha $n+1$ elementi ed è un sottoinsieme di G, che ha n elementi: obbligatoriamente, due elementi di X devono essere uguali.

Sia $g^r = g^s$ con $0 \leq r < s \leq n$. Moltiplicando r volte per g^{-1}, si ottiene $1_G = g^{s-r}$ e $s - r > 0$. Pertanto esiste almeno un intero i tale che $g^i = 1_G$ e quindi l'ordine di g è finito.

ii. Supponiamo che $g^r = g^s$. Come prima otteniamo $g^{s-r} = 1_G$. Si ha però che $0 < s - r < o(g)$ e questo contraddice la definizione di $o(g)$.

iii. Sia $o(g) = d$ e consideriamo il sottoinsieme di G dato da

$$S = \{1, g, g^2, \dots, g^{d-1}\}.$$

Per il punto precedente, $|S| = d$. Per un qualsiasi $h \in G$ definiamo

$$hS = \{h, hg, hg^2, \dots, hg^{d-1}\}.$$

È facile vedere che $|hS| = |S| = d$: se $hg^r = hg^s$ allora $g^r = g^s$.

Dimostriamo che se $h, k \in G$ allora

$$hS \cap kS = \varnothing \qquad \text{oppure} \qquad hS = kS. \tag{1.1}$$

Supponiamo che $hS \cap kS \neq \varnothing$ e siano $0 \leq r, s \leq d-1$ tali che $hg^r = kg^s$. Sia kg^i un qualsiasi elemento di kS. Da $hg^r = kg^s$ si ha $k = hg^{r-s}$ e pertanto $kg^i = hg^{r-s}g^i = hg^{r-s+i} \in hS$. Viceversa, sia hg^j un qualsiasi elemento di hS. Da $hg^r = kg^s$ si ha $h = kg^{s-r}$ e pertanto $hg^j = kg^{s-r}g^j = kg^{s-r+j} \in kS$ e questo completa la dimostrazione di 1.1.

Dalla proprietà 1.1 si ottiene che

$$G = \bigcup_{h \in G} hS$$

e l'unione è fatta in modo tale che due insiemi o sono disgiunti o sono uguali: scegliendo un opportuno insieme di rappresentanti R, possiamo quindi supporre che

$$G = \bigcup_{h \in R} hS$$

e questa volta l'unione è fatta di sottoinsiemi disgiunti, pertanto

$$n = |G| = \sum_{h \in R} |hS| = \sum_{h \in R} d = d \sum_{h \in R} 1 = d|R|$$

e quindi $d|n$.

iv. ($\Leftarrow$): sia $d = o(g)$ ed $m = dq$; allora

$$g^m = g^{dq} = (g^d)^q = 1_G^q = 1_G.$$

($\Rightarrow$): sia $m = dq + r$ con $0 < r < d$; allora

$$1_G = g^m = g^{dq+r} = g^{dq} g^r = (g^d)^q g^r = 1_G^q g^r = g^r$$

e questo contraddice la definizione di $d = o(g)$ come il più piccolo intero non nullo tale che $g^d = 1_G$ perché $0 < r < d$.

v. Moltiplicando $g^d = 1_G$ per g^{-1} e ripetendo ciò per d volte si ha $1_G = (g^{-1})^d$.

Se fosse $(g^{-1})^r = 1_g$ per un qualche r con $0 < r < d$, moltiplicando r volte per g otterremmo $1_G = g^r$, contro la definizione di $o(g)$.

vi. Sia $d = o(g_1 g_2)$, $d_1 = o(g_1)$ e $d_2 = o(g_2)$. Innanzi tutto, dal fatto che g_1 e g_2 commutano segue che

$$(g_1 g_2)^{d_1 d_2} = g_1^{d_1 d_2} g_2^{d_1 d_2} = (g_1^{d_1})^{d_2} (g_2^{d_2})^{d_1} = 1_G^{d_2} 1_G^{d_1} = 1_G$$

e pertanto $d|d_1 d_2$.

D'altra parte, da $(g_1 g_2)^d = 1_G$ segue che $g_1^d = (g_2^{-1})^d$. Ora, l'ordine di g_2^{-1} è uguale a d_2, l'ordine di g_2, e quindi

$$g_1^{dd_2} = (g_1^d)^{d_2} = ((g_2^{-1})^d)^{d_2} = ((g_2^{-1})^{d_2})^d = 1_G^d = 1_G,$$

che implica $d_1 = o(g_1)|dd_2$; ma $\mathrm{MCD}(d_1, d_2) = 1$ e, in definitiva, $d_1|d$.
In modo del tutto analogo si dimostra che $d_2|d$. Queste due proprietà, unite a $\mathrm{MCD}(d_1, d_2) = 1$, implicano che $d_1 d_2|d$ e quindi $d = d_1 d_2$.

□

Gli unici esempi di gruppi che ci capiterà di incontrare esplicitamente sono i gruppi abeliani moltiplicativi $\mathbb{Z}_n^*$ e K^*, dove K è un campo.

Capitolo 2

Anelli

In questo capitolo vedremo gli argomenti ed i risultati principali riguardanti gli anelli utili nel prosieguo.

Non entreremo nel dettaglio e di alcuni risultati non daremo la dimostrazione, rimandando eventualmente a testi di algebra: in realtà, noi saremo interessati solo al caso dei numeri interi ed al caso dei polinomi a coefficienti in un campo (finito). In tali casi, le nozioni che ci servono sono ben note (massimo comune divisore, fattorizzazione, ecc.) e verranno usate in modo "naif": non pretendiamo di aderire ad un formalismo rigoroso ed ineccepibile quale si addice ad un libro di testo di matematica ma piuttosto cercheremo di concentrarci sul lato "pratico", cioè computazionale ed algoritmico, degli argomenti che vedremo. Formalizzare tutti questi concetti richiede uno sforzo che ci porterebbe troppo lontano ed esula dallo scopo di queste note, per cui ci limitiamo a fornire le corrette definizioni e ad enunciare i risultati pertinenti, in modo da guidare il lettore interessato ad un approfondimento esterno: per ciò, si può consultare un qualsiasi libro di testo di algebra del Corso di Laurea in Matematica (per esempio, [11], [7], [3], [10]).

2.1 Anelli

In un insieme X, un'applicazione $f\colon X \times X \to X$ si chiama **operazione di composizione interna.** Un'operazione di composizione interna può essere considerata come un'operazione binaria nell'insieme: è una regola che prende due elementi, li "trasforma" e restituisce il risultato dell'operazione: $c = f(a, b)$. Dato che gli esempi più "elementari" di operazioni simili sono la somma ed il prodotto tra numeri, molto spesso si usa uno di tali simboli per indicare l'operazione: Per la somma, invece di scrivere $c = +(a, b)$ si scrive $c = a + b$; per il prodotto, invece, al posto di $c = \cdot(a, b)$ scriveremo $c = a \cdot b$ od anche $c = ab$.

DEFINIZIONE 2.1.1. *Un **anello**, che per noi sarà SEMPRE commutativo con unità tranne quando esplicitamente dichiarato altrimenti, è un insieme A con due operazioni di composizione interna, che indicheremo con "$+$" e "$\cdot$", e che soddisfano le seguenti proprietà:*

1. ***Proprietà associativa della somma:*** $\forall a, b, c \in A, \quad a + (b + c) = (a + b) + c$.

2. ***Elemento neutro della somma:*** $\exists! 0 \in A \quad t.c. \ \forall a \in A \quad 0+a = a+0 = a$.

3. ***Inverso della somma:*** $\forall a \in A \exists! -a \in A \quad t.c. \ a + (-a) = 0$.

4. ***Proprietà commutativa della somma:*** $\forall a, b \in A, \quad a + b = b + a$.

5. ***Proprietà associativa del prodotto:*** $\forall a, b, c \in A, \quad a(bc) = (ab)c$.

6. ***Elemento neutro del prodotto:*** $\exists! 1 \in A \quad t.c. \ \forall a \in A \quad 1a = a1 = a$.

7. ***Proprietà commutativa del prodotto:*** $\forall a, b \in A, \quad ab = ba$.

8. ***Proprietà distributiva:*** $\forall a, b, c \in A, \quad a(b + c) = ab + ac$.

DEFINIZIONE 2.1.2. *Un* ***campo*** *è un anello in cui vale anche la proprietà*

9. ***Inverso del prodotto:*** $\forall a \in A \setminus \{0\} \ \exists! a^{-1} \in A \quad t.c. \ aa^{-1} = 1$,

vale a dire, un anello in cui ogni elemento non nullo è invertibile.

DEFINIZIONE 2.1.3. *Un* ***dominio d'integrità*** *è un anello in cui*

$$ab = 0 \Rightarrow (a = 0 \ \vee \ b = 0).$$

NOTAZIONE 2.1.4. *Con A^* indicheremo il sottoinsieme di A formato dagli elementi non nulli: $A^* = A \setminus \{0\}$.*

Esempi ben noti di anelli sono gli insiemi di numeri $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ e $\mathbb{C}$. A parte $\mathbb{Z}$, questi anelli sono anche dei campi.

Un anello è anche l'insieme delle matrici quadrate di dimensione fissata, dove la somma è data componente per componente, mentre il prodotto è fatto riga per colonna. In questo caso, però, non vale la proprietà commutativa del prodotto.

Un altro esempio noto è quello dell'anello dei polinomi a coefficienti in un anello.

DEFINIZIONE 2.1.5. *Un elemento a di un anello A.*

1. *a si dice* ***divisore*** *di $b \in A$ se $\exists a' \in A$ tale che $aa' = b$; equivalentemente, si dice anche che b è* ***multiplo*** *di a. La notazione usata è $a|b$; l'elemento a' può anche essere indicato convenzionalmente con $\frac{b}{a}$.*

   Osserviamo che se non si richiede che a sia non nullo, allora ogni elemento è divisore di 0, dato che $a0 = 0$.

2. *a si dice* ***invertibile*** *se esiste un elemento $b \in A$ tale che $ab = 1$; l'insieme degli elementi invertibili di A viene indicato con $U(A)$.*

3. *a si dice* ***associato*** *a b (e scriveremo $a \sim b$) se esiste c invertibile tale che $a = bc$.*

4. *a si dice* ***primo*** *se è non nullo, non invertibile e*

$$a|bc \Rightarrow (a|b \quad oppure \quad a|c).$$