ALGEBRA I: SOLUZIONI QUINTA ESERCITAZIONE
9 maggio 2011

Esercizio 1. Usando l'algoritmo euclideo delle divisioni successive, calcolare massimo comune divisore e identità di Bézout per le seguenti coppie in $\mathbb{Z}[i]$:

$$(5+2i, 3-i), \qquad (7+i, 9+7i), \qquad (5+4i, 3+4i).$$

Soluzione. i) Calcoliamo le norme complesse dei due interi di Gauss e dividiamo quello di norma maggiore per quello di norma minore. Poiché

$$N(5+2i) = 25+4 = 29 \qquad \text{e} \qquad N(3-i) = 9+1 = 10,$$

dividiamo $5+2i$ per $3-i$ in $\mathbb{C}$:

$$\frac{5+2i}{3-i} = \frac{(5+2i)(3+i)}{10} = \frac{13}{10} + \frac{11}{10}i.$$

Pertanto l'intero di Gauss che meglio approssima il numero complesso $\frac{5+2i}{3-i}$ è $1+i$ e il resto della divisione euclidea di $5+2i$ per $3-i$ in $\mathbb{Z}[i]$ è 1, vale a dire

$$5+2i = (3-i)(1+i)+1 :$$

segue in particolare che $\mathrm{MCD}(5+2i, 3-i) = 1$ e che $1 = 5+2i-(3-i)(1+i)$ è l'identità di Bézout.

ii) Calcolando le norme complesse otteniamo

$$N(7+i) = 49+1 = 50 \qquad \text{e} \qquad N(9+7i) = 81+49 = 130,$$

dividiamo dunque $9+7i$ per $7+i$ in $\mathbb{C}$:

$$\frac{9+7i}{7+i} = \frac{(9+7i)(7-i)}{50} = \frac{7}{5} + \frac{4}{5}i.$$

Pertanto il quoziente della divisione euclidea di $9+7i$ per $7+i$ in $\mathbb{Z}[i]$ è $1+i$ e otteniamo

$$9+7i = (7+i)(1+i)+3-i.$$

Passiamo alla divisione successiva, vale a dire dividiamo $7+i$ per $3-i$. Effettuando la divisione in $\mathbb{C}$ otteniamo

$$\frac{7+i}{3-i} = \frac{(7+i)(3+i)}{10} = 2+i.$$

Pertanto $7+i$ è divisibile per $3-i$ in $\mathbb{Z}[i]$ ed otteniamo $\mathrm{MCD}(9+7i, 7+i) = 3-i$, mentre l'identità di Bézout è fornita dalla prima divisione:

$$3-i = (9+7i) - (1+i)(7+i).$$

iii) Calcolando le norme complesse otteniamo

$$N(5+4i) = 25+16 = 41 \qquad \text{e} \qquad N(3+4i) = 9+16 = 25,$$

dividiamo dunque $5+4i$ per $3+4i$ in $\mathbb{C}$:

$$\frac{5+4i}{3+4i} = \frac{(5+4i)(3-4i)}{25} = \frac{31}{25} - \frac{8}{25}i.$$

Pertanto otteniamo che il risultato della divisione euclidea di $5+4i$ per $3+4i$ in $\mathbb{Z}[i]$ è

$$5+4i = (3+4i)+2.$$

Dividiamo ora $3+4i$ per 2. Effettuando la divisione in $\mathbb{C}$ otteniamo

$$\frac{3+4i}{2} = \frac{3}{2} + 2i,$$

pertanto il risultato della divisione euclidea di $3+4i$ per 2 in $\mathbb{Z}[i]$ è

$$3+4i = 2(1+2i)+1.$$

Dunque $\mathrm{MCD}(9+7i, 7+i) = 1$ e risalendo nelle divisioni successive otteniamo l'identità di Bézout

$$1 = (2+2i)(3+4i) - (1+2i)(5+4i).$$

Esercizio 2. Se $z = a+bi \in \mathbb{Z}[i]$, si denoti $N(z) = a^2+b^2$ la sua norma complessa.

i) Mostrare che z è invertibile se e solo se $N(z) = 1$.

ii) Mostrare che se $N(z)$ è un numero primo, allora z è irriducibile. Mostrare con un controesempio che il viceversa è falso.

Soluzione. i) Sia $z \in \mathbb{Z}[i]$ un elemento invertibile: dall'uguaglianza $N(z)N(z^{-1}) = N(zz^{-1}) = 1$ segue che $N(z)$ è un intero positivo invertibile, vale a dire deve essere $N(z) = 1$. Viceversa, sia $z \in \mathbb{Z}[i]$ di norma 1. Detto $z = a+bi$, dalla definizione della norma otteniamo $a^2+b^2 = 1$: pertanto uno tra a e b è nullo, mentre l'altro è uguale a 1 o -1. Pertanto z è uno dei seguenti interi di Gauss, i quali sono tutti invertibili: $1, -1, i, -i$.

ii) Sia $z \in \mathbb{Z}[i]$ tale che $N(z)$ è un numero primo e supponiamo che $z = z_1z_2$ con $z_1, z_2 \in \mathbb{Z}[i]$. Passando alle norme, otteniamo l'uguaglianza $N(z) = N(z_1)N(z_2)$. Poiché $N(z)$ è un numero primo, uno tra $N(z_1)$ e $N(z_2)$ deve essere 1: dal punto i) otteniamo allora che uno tra z_1 e z_2 è invertibile. Pertanto z non ammette fattorizzazioni non banali ed è irriducibile.

Per mostrare che il viceversa non vale, si consideri $3 \in \mathbb{Z}[i]$ e mostriamo che è irriducibile. Siano $z_1, z_2 \in \mathbb{Z}[i]$ tali che $3 = z_1z_2$: allora considerando le norme otteniamo $N(z_1)N(z_2) = 9$. Se la fattorizzazione non è banale, deve neccessariamente essere $N(z_1) = N(z_2) = 3$: infatti altrimenti uno dei due fattori avrebbe norma 1 e sarebbe invertibile per il punto i). Per concludere che 3 è irriducibile, basta osservare che non esistono coppie di interi positivi a, b tali che $3 = a^2+b^2$. D'altra parte $N(3) = 9$ non è un numero primo, ed abbiamo mostrato che l'irriducibilità di un intero di Gauss non implica l'irriducibilità della sua norma.

Esercizio 3. Siano m, n due numeri interi.

i) Mostrare che m divide n in $\mathbb{Z}$ se e solo se m divide n in $\mathbb{Z}[i]$.

ii) Mostrare che il massimo comune divisore di m e n in $\mathbb{Z}$ coincide con il loro massimo comune divisore in $\mathbb{Z}[i]$.

Soluzione. i) Il fatto che la divisibilità in $\mathbb{Z}$ implica quella in $\mathbb{Z}[i]$ segue immediatamente dal fatto che $\mathbb{Z}$ è un sottoanello di $\mathbb{Z}[i]$. Supponiamo viceversa che m divide n in $\mathbb{Z}[i]$ e sia $a+bi$ il quoziente della divisione. Dunque

$$n = m(a+bi) = ma+mbi$$

e otteniamo $mb = 0$. Pertanto uno tra m e b è nullo, e in entrambi casi il risultato segue.

ii) Facciamo prima di tutto una considerazione di carattere generale.

Lemma. *Sia A un dominio a ideali principali e siano $a, b, d \in A$. Allora $d = \mathrm{MCD}(a, b)$ se e solo valgono le seguenti proprietà:*

D1) *d divide a e d divide b (vale a dire d è un divisore comune);*

D2) *Esistono $h, k \in A$ tali che $d = ha+kb$ (vale a dire esiste un'identità di Bézout).*

Dimostrazione. Supponiamo che d soddisfa D1) e D2) e sia c un divisore comune di a e b. Allora c divide ogni elemento della forma $xa+yb$ con $x, y \in A$: in particolare dunque c divide d. Viceversa, $\mathrm{MCD}(a, b)$ soddisfa D1) e D2): infatti esso è il generatore dell'ideale (a, b) generato da a e b, dunque esiste un'identità di Bézout. □

Osservazione Si osservi che se A è un dominio a fattorizzazione unica che non è a ideali principali (questo è il caso p.e. se $A = \mathbb{Z}[x]$ o $A = \Bbbk[x, y]$, dove $\Bbbk$ è un campo), allora il massimo comune divisore di due elementi è sempre ben definito ed unico a meno di invertibili, ma in generale non soddisfa la condizione D2): in effetti, il massimo comune divsore di a, b soddisfa D2) se e solo se l'ideale (a, b) è principale. Ad esempio in $\mathbb{Z}[x]$ l'ideale $(2, x)$ non è principale e $\mathrm{MCD}(2, x) = 1$, mentre in $\Bbbk[x, y]$ l'ideale (x, y) non è principale e $\mathrm{MCD}(x, y) = 1$: in entrambi questi casi, non esistono identità di Bézout per il massimo comune divisore della data coppia di elementi.

Usando il lemma precedente, per concludere l'esercizio è sufficiente osservare che, se d è il massimo comune divisore di m e n in $\mathbb{Z}$, allora d divide n e m in $\mathbb{Z}$ ed esiste un'identità di Bézout a coefficienti interi. In particolare, d divide n e m in $\mathbb{Z}[i]$ ed esiste un'identità di Bézout in $\mathbb{Z}[i]$, pertanto d coincide con il massimo comune divisore di m e n come interi di Gauss.

Osservazione Più in generale, una dimostrazione identica prova che se A è un dominio a ideali principali e se $B \subset A$ è un sottoanello che è a sua volta un dominio a ideali principali, allora il massimo comune divisore in B coincide con la restrizione del massimo comune divisore in A.

Esercizio 4. Sia $\mathbb{Z}[\sqrt{-3}]$ il sottoanello del campo dei numeri complessi definito da

$$\mathbb{Z}[\sqrt{-3}] = \{a + b\sqrt{-3} \ : \ a, b \in \mathbb{Z}\}.$$

Se $z = a + b\sqrt{-3}$, si denoti $N(z) = a^2 + 3b^2$ la sua norma complessa.

i) Dimostrare che un elemento $z \in \mathbb{Z}[\sqrt{-3}]$ è invertibile se e solo se $N(z) = 1$.

ii) Dimostrare che 2 e $1 + \sqrt{-3}$ sono elementi irriducibili.

iii) Usando l'uguaglianza

$$4 = 2 \cdot 2 = (1 + \sqrt{-3})(1 - \sqrt{-3})$$

dimostrare che 2 e $1 + \sqrt{-3}$ non sono elementi primi.

iv) Dedurre che $\mathbb{Z}[\sqrt{-3}]$ non è un dominio a ideali principali.

Soluzione. i) Come nel punto i) dell'Esercizio 2 si mostra che se $z \in \mathbb{Z}[\sqrt{-3}]$ è invertibile allora vale $N(z) = 1$. Viceversa, se a, b sono numeri interi tali che $N(a+b\sqrt{-3}) = 1$, allora da $a^2+3b^2 = 1$ si ricava che $a = 1, b = 0$ oppure $a = -1, b = 0$. D'altra parte 1 e -1 sono entrambi invertibili in $\mathbb{Z}[\sqrt{-3}]$, dunque segue i).

ii) Sia $2 = z_1 z_2$ una fattorizzazione non banale di 2 in $\mathbb{Z}[\sqrt{-3}]$. Passando alle norme si ottiene $N(z_1)N(z_2) = 4$: per il punto i), il fatto che la fattorizzazione non è banale implica allora $N(z_1) = N(z_2) = 2$. Ragionando come al punto i) è facile vedere che $\mathbb{Z}[\sqrt{-3}]$ non contiene elementi di norma 2, segue pertanto che 2 è irriducibile. Analogamente si mostra che $1 + \sqrt{-3}$ è irriducibile.

iii) Consideriamo l'uguaglianza

$$4 = 2 \cdot 2 = (1 + \sqrt{-3})(1 - \sqrt{-3}) :$$

per dedurre che 2 non è primo, è sufficiente mostrare che 2 non divide né $1 + \sqrt{-3}$ né $1 - \sqrt{-3}$. Supponiamo ad esempio

$$1 + \sqrt{-3} = 2z$$

per qualche $z \in \mathbb{Z}[\sqrt{-3}]$. Poiché $N(2) = N(1 + \sqrt{-3}) = 4$, passando alle norme otteniamo che deve necessariamente essere $N(z) = 1$. D'altra parte, come mostrato nel punto i), gli unici elementi di norma 1 in $\mathbb{Z}[\sqrt{-3}]$ sono 1 e -1, e pertanto otterremmo $1 + \sqrt{-3} = 2$ oppure $1 + \sqrt{-3} = -2$, che è assurdo: pertanto $2 \in \mathbb{Z}[\sqrt{-3}]$ è un elemento irriducibile ma non primo. Con ragionamento analogo si mostra che anche $1 + \sqrt{-3}$ e $1 - \sqrt{-3}$ sono irriducibili ma non primi.

iv) Poiché in un dominio a ideali principali ogni elemento irriducibile è primo, il punto iii) mostra che $\mathbb{Z}[\sqrt{-3}]$ non è un dominio a ideali principali. Equivalentemente, l'uguaglianza

$$4 = 2 \cdot 2 = (1 + \sqrt{-3})(1 - \sqrt{-3})$$

mostra che in $\mathbb{Z}[\sqrt{-3}]$ esistono fattorizzazioni non equivalenti, vale a dire che $\mathbb{Z}[\sqrt{-3}]$ non è un dominio a fattorizzazione unica.

Esercizio 5. Si denoti $\mathbb{F}_2 = \mathbb{Z}/(2)$ il campo con due elementi e si consideri il polinomio

$$x^3 + x + 1 \in \mathbb{F}_2[x].$$

Mostare che l'anello quoziente $\mathbb{F}_2[x]/(x^3 + x + 1)$ è un campo.

Soluzione. Si osservi che il polinomio $p(x) = x^3 + x + 1$ non possiede radici in $\mathbb{F}_2$:infatti $p(0) = p(1) = 1$. Questo implica che $p(x)$ è irriducibile. Se infatti $p(x) = q_1(x)q_2(x)$ fosse una fattorizzazione non banale, allora sarebbe $\deg(q_1) + \deg(q_2) = \deg(p)$, con $\deg(q_1) > 0$ e $\deg(q_2) > 0$: dunque uno tra $q_1(x)$ e $q_2(x)$ avrebbe grado 1, e $p(x)$ avrebbe una radice in $\mathbb{F}_2$.

La proiezione al quoziente $\mathbb{F}_2[x] \to \mathbb{F}_2[x]/(x^3 + x + 1)$ induce una corrispondenza biunivoca tra gli ideali di $\mathbb{F}_2[x]/(x^3 + x + 1)$ gli ideali di $\mathbb{F}_2[x]$ che contengono $(x^3 + x + 1)$. D'altra parte, poiché $x^3 + x + 1$ è irriducibile, esso genera un ideale massimale in $\mathbb{F}_2[x]$: pertanto gli unici ideali che lo contengono sono quelli banali (x^3+x+1) e $\mathbb{F}_2[x]$. Questo mostra che $\mathbb{F}_2[x]/(x^3+x+1)$ non possiede ideali non banali, dunque è un campo.

Osservazione. La stessa dimostrazione mostra più in generale che se $\Bbbk$ è un campo e $p \in \Bbbk[x]$ è un polinomio irriducibile, allora il quoziente $\Bbbk[x]/(p)$ è un campo.

Esercizio 6. Una *serie formale* a coefficienti in un campo $\Bbbk$ è una somma formale $\sum_{i=1}^{\infty} a_i x^i$, dove x è un'indeterminata e dove $a_i \in \Bbbk$ per ogni $i \geq 0$. Si denoti con $\Bbbk[[x]]$ l'insieme delle serie formali a coefficienti in $\Bbbk$, dotato della struttura di anello con le seguenti operazioni (che estendono quelle definite tra polinomi):

$$\sum_{i=0}^{\infty} a_i x^i + \sum_{i=0}^{\infty} b_i x^i = \sum_{i=0}^{\infty} (a_i + b_i) x^i, \qquad \left(\sum_{i=0}^{\infty} a_i x^i\right)\left(\sum_{i=0}^{\infty} b_i x^i\right) = \sum_{i=0}^{\infty} \Big(\sum_{j=0}^{i} a_j b_{i-j}\Big) x^i.$$

Data una serie formale non nulla $a(x) = \sum a_i x^i$, si definisca la sua *norma euclidea* come

$$\partial(a) = \min\{i \geq 0 \ : \ a_i \neq 0\}.$$

i) Mostare che un elemento non nullo $a(x) \in \Bbbk[[x]]$ è invertibile se e solo se $\partial(a) = 0$.

ii) Mostrare che, dati $a(x), b(x) \in \Bbbk[[x]]$ non nulli, allora $\partial(ab) = \partial(a) + \partial(b)$.

iii) Mostrare che, dati $a(x), b(x) \in \Bbbk[[x]]$ non nulli, allora a divide b se e solo se $\partial(a) \leq \partial(b)$.

iv) Dedurre che $\Bbbk[[x]]$ è un dominio euclideo.

Soluzione. i) Sia $\sum a_i x^i \in \Bbbk[[x]]$ con $a_0 \neq 0$, mostriamo che una tale serie è invertibile. Equivalentemente, vogliamo definire una seconda serie $\sum b_i x^i$ tale che

$$\left(\sum_{i=1}^{\infty} a_i x^i\right)\left(\sum_{i=1}^{\infty} b_i x^i\right) = 1.$$

Dalla definizione del prodotto in $\Bbbk[[x]]$, otteniamo il seguente sistema infinito di equazioni:

$$\begin{cases} a_0 b_0 = 1 \\ a_0 b_1 + a_1 b_0 = 0 \\ a_0 b_2 + a_1 b_1 + a_2 b_0 = 0 \\ \ldots\ldots\ldots\ldots \\ \sum_{k=1}^{i} a_k b_{i-k} = 0 \\ \ldots\ldots\ldots\ldots \end{cases}$$

Pertanto possiamo definire ricorsivamente la serie inversa $\sum b_i x^i$ come segue:

$$\begin{cases} b_0 = \frac{1}{a_0} \\ b_1 = -\frac{a_1 b_0}{a_0} \\ b_2 = -\frac{a_1 b_1 + a_2 b_0}{a_0} \\ \ldots\ldots\ldots\ldots \\ b_i = -\frac{\sum_{k=1}^{i-1} a_k b_{i-k}}{a_0} \\ \ldots\ldots\ldots\ldots \end{cases}$$

ii) Poniamo $a(x) = \sum a_i x^i$ e $b(x) = \sum b_i x^i$. Se $a(x)b(x) = \sum c_i x^i$, allora dalla definizione del prodotto in $\Bbbk[[x]]$ otteniamo $c_i = 0$ per ogni $i < \partial(a) + \partial(b)$. In effetti se $j < \partial(a)$ allora $a_j = 0$, mentre se $\partial(a) \leq j < \partial(b)$ allora $i - j < \partial(b)$ e $b_{i-j} = 0$: pertanto

$$c_i = \sum_{j=0}^{i} a_j b_{i-j} = 0$$

e $\partial(ab) \geq \partial(a) + \partial(b)$. D'altra parte similmente si mostra $c_{\partial(a)+\partial(b)} = a_{\partial(a)} b_{\partial(b)}$, dunque $\partial(ab) = \partial(a) + \partial(b)$.

iii) Poniamo $a(x) = \sum a_i x^i$ e $b(x) = \sum b_i x^i$. Se $\partial(b) < \partial(a)$, allora segue dal punto ii) che $a(x)$ non può dividere $b(x)$. Supponiamo dunque $\partial(b) \geq \partial(a)$ e, sfruttando il punto i), mostriamo che $a(x)$ divide $b(x)$.

Poniamo $d = \partial(a)$ e mettiamo in evidenza il termine x^d in $a(x)$ e $b(x)$: dunque $a(x) = x^d a_0(x)$ e $b(x) = x^d b_0(x)$, dove $a_0(x), b_0(x) \in \Bbbk[[x]]$. Dalla definizione di d otteniamo che $\partial(a') = 0$: il punto i) implica allora che $a_0(x)$ ammette inverso in $\Bbbk[[x]]$. Pertanto possiamo scrivere

$$b(x) = x^d b'(x) = x^d b'(x) a_0^{-1}(x) a_0(x) = \big(b'(x) a_0^{-1}(x)\big)\big(x^d a_0(x)\big) = c(x)a(x),$$

dove $c(x) \in \Bbbk[[x]]$ è la serie formale definita da $c(x) = b'(x)a_0^{-1}(x)$: quindi $a(x)$ divide $b(x)$.

iv) Dal punto ii) segue che l'applicazione $\partial : \Bbbk[[x]] \smallsetminus \{0\} \longrightarrow \mathbb{N}$ soddisfa la disuguaglianza $\partial(a) \leq \partial(ab)$. Dati $a(x), b(x) \in \Bbbk[[x]]$, definiamo il quoziente $q(x)$ e il resto $r(x)$ della divisione di $a(x)$ per $b(x)$ come segue:

$$q(x) = \begin{cases} a(x)/b(x) & \text{se } \partial(b) \leq \partial(a) \\ 0 & \text{se} \partial(b) > \partial(a) \end{cases} \qquad r(x) = \begin{cases} 0 & \text{se } \partial(b) \leq \partial(a) \\ a(x) & \text{se } \partial(b) > \partial(a) \end{cases}$$

dove, se $\partial(b) \leq \partial(a)$, con $a(x)/b(x)$ indichiamo il risultato della divisione di $a(x)$ per $b(x)$ (che è ben definito grazie al punto iii)). Segue quindi dalla definizione di $q(x)$ e $r(x)$ che

$$a(x) = b(x)q(x) + r(x)$$

con $\partial(r) < \partial(b)$ oppure $r = 0$.

Osservazione In effetti l'anello $\Bbbk[[x]]$ è molto più di un dominio euclideo: esso è un *dominio a valutazione discreta*. Tali anelli possiedono notevoli proprietà, illustriamone alcune nel nostro esempio. Ad esempio, gli ideali di $\Bbbk[[x]]$ hanno una descrizione molto elegante: essi sono tutti della forma (x^d) per qualche $d \in \mathbb{N}$. Più precisamente, se $I \subset \Bbbk[[x]]$ è un ideale non nullo e se

$$d = \min\{\partial(p) \,:\, p(x) \in I\},$$

allora è facile vedere che $I = (x^d)$. Sia infatti $p(x) \in I$ tale che $\partial(p) = d$: allora $x^d \in I$ perché $p(x)$ divide x^d grazie al punto iii), mentre - di nuovo grazie al punto iii) - ogni elemento di I è divisibile per x^d. Detto altrimenti,

$$I = \{p \in \Bbbk[[x]] \,:\, \partial(p) \geq d\}$$

ed è generato da qualsiasi suo elemento di norma d.

Dunque abbiamo mostrato che l'insieme degli ideali di $\Bbbk[[x]]$ ha la seguente struttura ordinata:

$$\Bbbk[[x]] = (1) \supset (x) \supset (x^2) \supset \ldots \supset (x^d) \supset \ldots$$

Seguono i seguenti fatti:

- $\Bbbk[[x]]$ possiede un unico ideale massimale, che coincide con l'ideale costituto dalle serie formali di norma maggiore o uguale a 1 (il fatto di avere un unico ideale massimale è un'importante proprietà per un anello, che gli vale il nome di *anello locale*);
- gli elementi primi di $\Bbbk[[x]]$ coincidono con le serie formali di norma 1: essi sono tutti associati tra di loro (vale a dire differiscono per un fattore di norma 0) e generano tutti lo stesso ideale;
- l'insieme degli elementi invertibili di $\Bbbk[[x]]$ coincide con il complementare dell'unico ideale massimale.