Lezione 11

Prerequisiti: Lezione 10.

Polinomi a coefficienti in un campo.

Sia K un campo. In questa lezione studiamo le proprietà aritmetiche dell'anello di polinomi $K[X]$, che sono analoghe a quelle valide nell'anello $\mathbb{Z}$ e da noi considerate nelle Lezioni 6 e 7.
Le loro dimostrazioni, laddove esse siano simili a quelle già effettuate per i numeri interi, verranno qui omesse.

Ricordiamo che, nella Lezione 6, abbiamo definito la relazione di divisibilità in ogni anello commutativo unitario (v. Definizione 6.1). Questa si applica, in particolare, all'anello $K[X]$. Ad essa si riferisce l'intero contenuto di questa lezione, a cominciare dal primo enunciato, che è analogo al Teorema 6.10.

Sarà inoltre utile tenere presente che, come conseguenza del Corollario 5.18 e del Corollario 10.6, l'anello $K[X]$ è integro.

Teorema 11.1 *(Teorema di divisione euclidea)* Siano $a(X), b(X) \in K[X]$, ove $b(X) \neq 0$. Allora esistono, e sono univocamente determinati, $q(X), r(X) \in K[X]$ tali che
(i) $a(X) = b(X)q(X) + r(X)$;
(ii) $r(X) = 0$ oppure $r(X) \neq 0$ e $\deg(r) < \deg(b)$.

I polinomi $q(X)$ ed $r(X)$ si dicono, rispettivamente, *quoziente* e *resto* della *divisione (euclidea)* di $a(X)$ per $b(X)$. I polinomi $a(X)$ e $b(X)$ si dicono, rispettivamente, *dividendo* e *divisore*.

Dimostrazione: Proviamo prima l'esistenza. A tal fine consideriamo l'insieme

$$C = \{a(X) - b(X)f(X) \mid f(X) \in K[X]\}.$$

Se $0 \in C$, allora esiste $q(X) \in K[X]$ tale che $a(X) - b(X)q(X) = 0$ e la tesi è verificata con $r(X) = 0$. Supponiamo ora che $0 \notin C$. Sia D l'insieme dei gradi dei polinomi di C. Allora D è un sottoinsieme non vuoto di $\mathbb{N}$. Quindi, per il principio del minimo (assioma di buon ordinamento), D possiede un minimo d. Sia $r(X) \in C$ tale che $\deg(r) = d$. Allora $a(X) - b(X)q(X) = r(X)$ per qualche $q(X) \in K[X]$ e dunque è verificata la condizione (i). Poiché $r(X) \neq 0$, resta da provare che $d < \deg(b)$. Supponiamo per assurdo che $d \geq \deg(b)$. Sia $n = \deg(b)$ e siano

$$r(X) = \sum_{i=0}^{d} r_i X^i, \quad b(X) = \sum_{i=0}^{n} b_i X^i, \quad (r_i, b_i \in K).$$

Sia ora $r'(X) = r(X) - r_d b_n^{-1} X^{d-n} b(X) = a(X) - b(X)(q(X) + r_d b_n^{-1} X^{d-n}) \in C$. Allora $r'(X) \neq 0$ e

$$r'(X)=\sum_{i=0}^{d} r_i X^i - r_d b_n^{-1} X^{d-n}\sum_{i=0}^{n} b_i X^i = \underbrace{r_d X^d - r_d b_n^{-1} X^{d-n} b_n X^n}_{0} + \underbrace{\sum_{i=0}^{d-1} r_i X^i - r_d b_n^{-1}\sum_{i=0}^{n-1} b_i X^{d-n+i}}_{\deg<d}.$$

Quindi $\deg(r')<d$, contro la minimalità di d. Ciò fornisce la contraddizione cercata e conclude la dimostrazione dell'esistenza di $q(X),r(X)\in K[X]$ verificanti la (i) e la (ii).
Proviamo ora l'unicità. Siano $q_1(X),q_2(X),r_1(X),r_2(X)\in K[X]$ tali che $q(X)=q_i(X),r(X)=r_i(X)$ con $i=1,2$, verificano la (i) e la (ii). Allora, in particolare,

$$b(X)q_1(X)+r_1(X)=b(X)q_2(X)+r_2(X), \tag{1}$$

da cui $b(X)(q_1(X)-q_2(X))=r_2(X)-r_1(X)$. Supponiamo per assurdo che sia $r_2(X)-r_1(X)\neq 0$. Allora, uno tra $r_1(X),r_2(X)$ è non nullo. Sia esso $r_2(X)$. Se anche $r_1(X)$ è non nullo, sia $r_2(X)$ quello tra i due che ha grado massimo. Allora, in base alle formule del grado (Proposizione 10.2),

$$\deg(r_2)\geq\deg(r_2-r_1)=\deg(b(q_1-q_2))=\deg(b)+\deg(q_1-q_2)\geq\deg(b)$$

Ma allora $\deg(r_2)\geq\deg(b)$, contro la (ii). Quindi $r_1(X)=r_2(X)$, e dalla (1) segue che $q_1(X)=q_2(X)$. Ciò prova l'unicità del quoziente e del resto. □

Esempio 11.2 Per determinare il quoziente ed il resto della divisione euclidea del polinomio $a(X)$ per il polinomio $b(X)$ si può effettuare una divisione in colonna. Consideriamo ad esempio, in $\mathbb{Q}[X]$, i polinomi $a(X)=X^4+X-2$ e $b(X)=2X^3+X^2$.

$$\begin{array}{rrrrrrr|l|lll}
X^4 & & & + & X & - & 2 & 2X^3+X^2 & & \\
\hline
X^4 & + & \frac{1}{2}X^3 & & & & & \frac{1}{2}X-\frac{1}{4} & = & q(X) \\
\hline
 & - & \frac{1}{2}X^3 & & + & X & - 2 & & & \\
 & - & \frac{1}{2}X^3 & - & \frac{1}{4}X^2 & & & & & \\
\hline
 & & & & \frac{1}{4}X^2 & + & X - 2 & & = & r(X)
\end{array}$$

Abbiamo ottenuto il quoziente $q(X)=\frac{1}{2}X-\frac{1}{4}$ ed il resto $r(X)=\frac{1}{4}X^2+X-2$.

Definiamo ora la nozione di massimo comune divisore in $K[X]$: essa è analoga a quella data in $\mathbb{Z}$ (v. Definizione 6.13). Si potrà dare, in maniera simile, una definizione di minimo comune multiplo.

Definizione 11.3 Siano $a(X),b(X)\in K[X]$. Allora si dice *massimo comune divisore* di $a(X)$ e $b(X)$ ogni polinomio $d(X)$ tale che
(a) $d(X)\mid a(X)$ e $d(X)\mid b(X)$;
(b) per ogni $e(X)\in K[X]$ tale che $e(X)\mid a(X)$ ed $e(X)\mid b(X)$, si ha che $e(X)\mid d(X)$.

Dati $a(X), b(X) \in K[X]$, esiste sempre un loro massimo comune divisore. Ciò segue dal prossimo enunciato, analogo alla Proposizione 6.15. La sua dimostrazione, che non riportiamo per brevità, si basa, come nel caso dell'anello $\mathbb{Z}$, sul Teorema di divisione euclidea e sfrutta il principio del minimo, applicato ad insiemi i cui elementi sono gradi di polinomi verificanti una certa proprietà. In altri termini, la dimostrazione del prossimo enunciato si effettua operando, sulla dimostrazione della Proposizione 6.15, modifiche analoghe a quelle che hanno prodotto la dimostrazione del Teorema 11.1 a partire da quella del Teorema 6.10.

Proposizione 11.4 *(Lemma di Bézout)* Siano $a(X), b(X) \in K[X]$. Allora esiste un massimo comune divisore $d(X)$ di $a(X)$ e $b(X)$. Inoltre esistono $s(X), t(X) \in K[X]$ tali che

$$s(X)a(X) + t(X)b(X) = d(X). \tag{2}$$

Tale uguaglianza si dice *identità di Bézout*. I polinomi $s(X), t(X)$ si dicono *coefficienti di Bézout* di $a(X)$ e $b(X)$.

Come per i numeri interi, i massimi comuni divisori di due polinomi fissati sono a due a due associati. Il prossimo risultato è analogo alla Proposizione 6.16.

Proposizione 11.5 Siano $a(X), b(X) \in K[X]$ e sia $d(X)$ un massimo comune divisore di $a(X)$ e $b(X)$. Allora i massimi comuni divisori di $a(X)$ e $b(X)$ sono tutti e soli i polinomi $ud(X)$, ove $u \in K^*$.

Nota Si ha $d(X) = 0$ se e solo se $a(X) = b(X) = 0$. In tutti gli altri casi esiste uno ed un solo massimo comune divisore di $a(X)$ e $b(X)$ avente coefficiente direttore uguale a 1 (un polinomio siffatto si dice *monico*). Questo viene indicato con il simbolo $\mathrm{MCD}(a(X), b(X))$.

Anche in $K[X]$ i massimi comuni divisori si determinano con l'algoritmo delle divisioni successive, di cui proponiamo qui di seguito la versione per i polinomi.

Siano $a(X), b(X) \in K[X]$, entrambi non nulli. Si comincia effettuando la divisione con resto di $a(X)$ per $b(X)$:

1) $a(X) = b(X)q_1(X) + r_1(X)$ $\qquad (r_1(X) = 0$ oppure $r_1(X) \neq 0$ e $\deg(r_1) < \deg(b).)$

Se $r_1(X) \neq 0,$ si prosegue effettuando la divisione con resto di $b(X)$ per $r_1(X)$:

2) $b(X) = r_1(X)q_2(X) + r_2(X)$ $\qquad (r_2(X) = 0$ oppure $r_2(X) \neq 0$ e $\deg(r_2) < \deg(r_1).)$

Se $r_2(X) \neq 0,$ si prosegue effettuando la divisione con resto di $r_1(X)$ per $r_2(X)$:

3) $r_1(X) = r_2(X)q_3(X) + r_3(X).$ $\qquad (r_3(X) = 0$ oppure $r_3(X) \neq 0$ e $\deg(r_3) < \deg(r_2).)$

Fintanto che non si trova un resto nullo, si va avanti, ricorsivamente, effettuando ogni volta la divisione del penultimo resto per l'ultimo resto trovato. In questo modo, il passo i-esimo fornisce l'uguaglianza:

i.) $r_{i-2}(X) = r_{i-1}(X)q_i(X) + r_i(X)$ $\qquad$ ($r_i(X) = 0$ oppure $r_i(X) \neq 0$ e $\deg(r_i) < \deg(r_{i-1})$.)

In base a quanto osservato a margine delle uguaglianze 1.), 2.), 3.), …*i.*), (e che deriva dalla condizione (ii) del Teorema 11.1), si conclude che la sequenza dei gradi dei resti non nulli è strettamente decrescente:

$$\deg(r_1) > \deg(r_2) > \deg(r_3) > \cdots > \deg(r_i) > \cdots$$

Poiché questi numeri sono tutti maggiori o uguali a zero, la sequenza dei resti non nulli non può essere infinita. Quindi il nostro procedimento si conclude con le seguenti due uguaglianze:

n–1.) $r_{n-3}(X) = r_{n-2}(X)q_{n-1}(X) + r_{n-1}(X)$ $\qquad$ ($r_{n-1}(X) \neq 0$ e $\deg(r_{n-1}) < \deg(r_{n-2})$.)

n.) $r_{n-2}(X) = r_{n-1}(X)q_n(X)$

Si prova allora che $r_{n-1}(X)$ è un massimo comune divisore di $a(X)$ e $b(X)$; infatti vale la seguente proposizione, analoga alla Proposizione 6.18:

Proposizione 11.6 Un massimo comune divisore di due polinomi non nulli (che non siano uno divisore dell'altro) è l'ultimo resto non nullo che compare nel relativo algoritmo delle divisioni successive.

Esercizio 11.7* Siano, come nell'Esempio 11.2, $a(X) = X^4 + X - 2$ e $b(X) = 2X^3 + X^2$. Provare che $\mathrm{MCD}(a(X), b(X)) = 1$.

Nel resto di questa lezione presenteremo, in $K[X]$, nozioni analoghe a quelle viste nella Lezione 7.

Osserviamo preliminarmente che, in virtù del Corollario 10.7, i polinomi invertibili di $K[X]$ sono tutti e soli quelli costanti e non nulli (ossia, $U(K[X]) = K^*$), equivalentemente: i polinomi di grado zero.

I prossimi tre enunciati corrispondono, nell'ordine, alle Definizioni 7.1 e 7.2 e al Lemma 7.3.

Definizione 11.8 Un polinomio $p(X) \in K[X]$, non nullo e non invertibile, si dice *primo* se, per ogni $a(X), b(X) \in K[X]$,

$$p(X) \mid a(X)b(X) \Rightarrow p(X) \mid a(X) \quad \text{oppure} \quad p(X) \mid b(X).$$

Altrimenti $p(X)$ si dice *composto.*

Definizione 11.9 Un polinomio $p(X) \in K[X]$, non nullo e non invertibile, si dice *irriducibile* se, per ogni $a(X), b(X) \in K[X]$,

$$p(X) = a(X)b(X) \Rightarrow a(X) \text{ è invertibile oppure } b(X) \text{ è invertibile.}$$

Altrimenti $p(X)$ si dice *riducibile.*

Lemma 11.10 Sia $p(X)\in K[X]$ un polinomio non nullo e non invertibile. Allora sono equivalenti le seguenti condizioni.

(i) $p(X)$ è primo;
(ii) $p(X)$ è irriducibile;
(iii) i divisori di $p(X)$ sono tutti e soli i polinomi $u, up(X)$, ove $u\in K^*$.

Osservazione 11.11 Ricordiamo che, in base al Lemma 7.3, i divisori di un numero primo p sono $1,-1,p,-p$. Dal confronto con la condizione (iii) del Lemma 11.10 risulta che, sia nell'anello $\mathbb{Z}$, sia nell'anello $K[X]$ i divisori di un elemento primo (equivalentemente, irriducibile) sono tutti e soli gli elementi invertibili ed i prodotti tra questi e l'elemento stesso.
D'ora in poi sostituiremo la condizione *non nullo e non invertibile* con la condizione equivalente *non costante.* Inoltre useremo i termini *primo* ed *irriducibile* come sinonimi.

Il prossimo enunciato, analogo al Lemma 7.5, si deduce dalla Definizione 11.8 con un facile ragionamento induttivo.

Lemma 11.12* Sia $p(X)\in K[X]$ un polinomio primo e siano $a_1(X),...,a_r(X)\in K[X]$ tali che $p(X)\mid a_1(X)\cdots a_r(X)$. Allora $p(X)\mid a_i(X)$ per qualche $i\in\{1,...,r\}$.

Corollario 11.13 Sia $p(X)\in K[X]$. Se $\deg(p)=1$, allora $p(X)$ è irriducibile.

Dimostrazione: Siano $a(X),b(X)\in K[X]$ tali che $p(X)=a(X)b(X)$. Allora, in base alla formula del grado per il prodotto (Proposizione 10.2 (b)), segue che

$$\deg(p)=\deg(a)+\deg(b).$$

Dunque, se $\deg(p)=1$, allora $\{\deg(a),\deg(b)\}=\{0,1\}$. Dunque uno tra $a(X)$ e $b(X)$ ha grado zero, ossia $a(X)$ è invertibile oppure $b(X)$ è invertibile. Ciò prova che $p(X)$ è irriducibile. □

Esempio 11.14 I polinomi di grado maggiore di 1 non sono necessariamente irriducibili. Ad esempio, il polinomio quadratico $f(X)=X^2+3X+2\in\mathbb{Q}[X]$ è riducibile, poiché ammette la decomposizione

$$f(X)=(X+1)(X+2)$$

in cui nessuno dei due fattori a secondo membro è invertibile.

Nell'anello $K[X]$, come nell'anello $\mathbb{Z}$, vale un teorema di fattorizzazione unica, ossia un enunciato analogo al Teorema 7.6.

Teorema 11.15 *(Teorema di fattorizzazione unica)* Sia $f(X)\in K[X]$ un polinomio non costante. Allora esistono, per qualche intero positivo s, s polinomi irriducibili $p_1(X), p_2(X),..., p_s(X)\in K[X]$ tali che

$$f(X) = p_1(X)p_2(X)\cdots p_s(X). \tag{3}$$

Inoltre, il numero s ed i polinomi $p_1(X), p_2(X),..., p_s(X)$ sono univocamente determinati a meno di moltiplicazione per polinomi costanti non nulli.

Dimostrazione: Supponiamo per assurdo che esista polinomio non costante per il quale non esiste una decomposizione del tipo (3). Allora l'insieme C di tali polinomi è non vuoto. Sia D l'insieme dei gradi di tali polinomi; allora D è un sottoinsieme non vuoto di $\mathbb{N}$ ed in quanto tale, per il principio del minimo (assioma di buon ordinamento), ammette un minimo m. Sia $f(X) \in C$ tale che $\deg(f) = m$. In particolare $f(X)$ non è allora un polinomio irriducibile. Pertanto esistono $a(X), b(X) \in K[X]$ non invertibili tali che $f(X) = a(X)b(X)$. Allora $a(X), b(X)$ sono non nulli e di grado positivo. D'altra parte, in base alla formula del grado per il prodotto, $m = \deg(f) = \deg(a) + \deg(b)$, e quindi, essendo $\deg(a) > 0$, $\deg(b) < m$. Analogamente si deduce che $\deg(a) < m$. Dunque $a(X), b(X) \notin C$, quindi $a(X), b(X)$ si scrivono come prodotti di polinomi irriducibili, e quindi lo stesso vale per $f(X)$, contro l'ipotesi. Ciò prova che ogni polinomio non costante di $K[X]$ ammette una decomposizione del tipo (3). Supponiamo ora che il polinomio non costante $f(X) \in K[X]$ ammetta, oltre ad (3), la seguente decomposizione, dove t è un intero positivo e $q_1(X), q_2(X),..., q_t(X) \in K[X]$ sono polinomi irriducibili:

$$f(X) = q_1(X)q_2(X)\cdots q_t(X). \tag{4}$$

Proviamo allora che $s = t$ e che, a meno di riordinare i fattori in (3) e in (4), per ogni $i = 1,..., s$ si ha $p_i = u_i q_i$ per qualche $u_i \in K^*$. Procediamo per induzione su s. Se $s = 1$, allora $f(X) = p_1(X)$ è irriducibile. Dalla (4) segue allora che $t = 1$. Non può essere, infatti, $t \geq 2$, perché altrimenti $f(X)$ sarebbe il prodotto di $q_1(X)$ e $q_2(X)\cdots q_t(X)$, che sono polinomi non costanti e quindi non invertibili, e dunque $f(X)$ sarebbe riducibile. Quindi $f(X) = q_1(X)$, e pertanto, in particolare, $p_1(X) = q_1(X)$. Ciò prova la base dell'induzione. Supponiamo ora che sia $s > 1$ e che la tesi sia vera per $s-1$. Dalla (3) e dalla (4) segue che

$$p_1(X)p_2(X)\cdots p_s(X) = q_1(X)q_2(X)\cdots q_t(X). \tag{5}$$

Poiché $p_1(X)$ divide il prodotto a secondo membro, e $p_1(X)$ è primo, in virtù del Lemma 11.5, a meno di riordinare i fattori, si ha che $p_1(X) \mid q_1(X)$. Ma, in base al Lemma 11.10, i divisori di $q_1(X)$ sono tutti e soli i polinomi invertibili ed i prodotti di questi ultimi con $q_1(X)$. Essendo $p_1(X)$ non costante, segue che $p_1 = u_1 q_1$ per qualche $u_1 \in K^*$. Allora, essendo $p_1(X)$ non nullo e quindi cancellabile, dalla (5) segue che $p_2(X)\cdots p_s(X) = \widetilde{q_2}(X)\cdots q_t(X)$, ove $\widetilde{q_2}(X) = u_1^{-1} q_2(X)$ è associato a $q_2(X)$ (v. Proposizione 6.6) e quindi irriducibile (v. Corollario 6.8). Il numero di fattori a primo membro è $s-1$, mentre i fattori a secondo membro sono $t-1$, quindi, per l'ipotesi induttiva, si ha $s-1 = t-1$, cioè $s = t$, e, a meno di riordinare i fattori, per ogni $i = 2,..., s$, $p_i = u_i q_i$ per qualche $u_i \in K^*$.
Ciò conclude il passo induttivo e completa la dimostrazione. □

Nota L'uguaglianza (3) si dice *fattorizzazione* o *decomposizione in fattori irriducibili* del polinomio $f(X)$. I polinomi $p_i(X)$ (ed i polinomi ad essi associati) si dicono i *fattori irriducibili* di $f(X)$.

Esempio 11.16 Sia, come nell'Esempio 11.14, $f(X) = X^2 + 3X + 2 \in \mathbb{Q}[X]$. Allora $f(X)$ ammette le seguenti fattorizzazioni:

$$f(X) = (X+1)(X+2),\ f(X) = (-X-1)(-X-2),\ f(X) = (2X+2)(\frac{1}{2}X+1).$$

Queste sono solo tre delle infinite fattorizzazioni $f(X) = (aX + a)(a^{-1}X + 2a^{-1})$, ove $a \in \mathbb{Q}^*$.

Nel prossimo esercizio, di carattere teorico, si estende all'anello $K[X]$ la definizione di elementi coprimi (introdotta nella Definizione 6.20 per i numeri interi), e si richiede di adattare al caso dei polinomi le dimostrazioni del Corollario 6.21, della Proposizione 6.22 e lo svolgimento dell'Esercizio 7.11.

Esercizio 11.17* Siano $a(X), b(X) \in K[X]$. Provare che sono equivalenti le seguenti condizioni.

(i) $MCD(a(X), b(X)) = 1$;
(ii) esistono $s(X), t(X) \in K[X]$ tali che $s(X)a(X) + t(X)b(X) = 1$;
(iii) $a(X)$ e $b(X)$ non hanno fattori primi in comune.

Se valgono (i), (ii) e (iii), i polinomi $a(X)$ e $b(X)$ si dicono *coprimi.*